2024:DHC:8816

* **IN THE HIGH COURT OF DELHI AT NEW DELHI**

% **Judgment reserved on : 03 September 2024**
Judgment pronounced on : 18 November 2024

\+ W.P.(C) 13497/2022

HARE RAM SINGH .....Petitioner
Through: Mr. Ravi Chandra, Advocate.

versus

RESERVE BANK OF INDIA & ORS. ....Respondents
Through: Mr. Rajiv Kapur, Mr. Akshit Kapur, Ms. Riya, Advs. for R-2 and R3.
Mr. Abhinav Sharma, Adv. for RBI.

CORAM:
HON'BLE MR. JUSTICE DHARMESH SHARMA

J U D G M E N T

1. The petitioner herein invokes the writ jurisdiction of this Court under Article 226 of the Constitution of India, 1950, seeking the following reliefs against the respondents:

> "(i) Issue writ of *mandamus* or any other appropriate writ, Order or directions quashing the rejection order dated 26.07.2021 by SBI Branch Greater Noida (Annexure P/8 herein) as violative of Articles 14, 16 and 21 read with Article 300A of the Constitution of India read with RBI Master Circular dated 6.7.2017;
> (ii) Issue writ of *mandamus* or any other appropriate writ, Order or directions to the respondents to restore the amount illegally siphoned off from the Petitioner's SBI savings Account bearing No. 30051013904 IFSC Code: SBIN0004324 on 18/4/2021 by unknown 3rd Parties amounting to Rs 2,27,000/- with interest and;
> (iii) Pass any other necessary/appropriate directions in the matter as the Hon'ble Court may deem fit and proper in the interest of justice."

BRIEF FACTS:

2. Shorn of unnecessary details, the petitioner who is an academician aged about 55 years, became a victim of cyber fraud

perpetrated through a 'vishing attack' i.e., a voice-phishing attack wherein innocent people are enticed over voice-call to divulge sensitive information pertaining to their bank accounts, which information is then misused by the unscrupulous attacker so as to wrongfully enrich himself monetarily.

3. Shorn of unnecessary details, the petitioner on 18.04.2021 at about 05.15 PM, received an SMS[1] containing a link, upon receipt of which SMS he got a call from an unknown caller who convinced him to click on the said link contained in the SMS so as to keep the SMS service on his mobile number open and operational, and as soon as the unsuspecting petitioner clicked on the SMS link upon being prompted by the unknown caller/fraudster, an aggregate amount of Rs. 2,60,000/- was unauthorisedly withdrawn by way of two transactions in the sum of Rs. 1,00,000/- and Rs. 1,60,000/- each, from his Savings Bank Account maintained with the respondent Nos.2 and 3/State Bank of India **['SBI']** at its Greater Noida, Uttar Pradesh branch; and that on perusal of the statement of account of the petitioner, it was found that by way of internet banking on 18.04.2021, the first transaction of Rs. 1,00,000/- was made to a bank account maintained with IDFC Bank, and the second transaction of Rs. 1,60,000/- was made to One 97 Communications Ltd. (Paytm**)**.

4. Upon realising that he had been defrauded, the petitioner herein immediately dialled the 'Customer Care Department' of the SBI to register a complaint and seek a hold on the transactions that had been initiated without his permission, however to no avail. The petitioner

[1] Short Message Service

filed a complaint dated 20.04.2021 before the Branch Manager, SBI, Greater Noida besides filing a cyber complaint dated 18.04.2021 as well as complaint dated 19.04.2021 at PS Hajipur, Bihar, and also registering his grievance under the CPGRAMS[2] against the unauthorised withdrawal.

5. It is stated that since the grievance of the petitioner was not being redressed by the SBI, he filed a complaint dated 26.04.2021 before the Banking Ombudsman **['BO']** against the SBI for its inaction and failure to resolve the matter; and during the pendency of the complaint filed before the BO, the petitioner regularly served reminders upon the Chairman, SBI dated 02.05.2021, 21.05.2021, and 31.05.2021 seeking the updated status as regards the action taken upon his complaint. On 26.07.2021, the Chief Manager SBI, Greater Noida Branch, issued a letter to the petitioner, thereby rejecting the petitioner's complaint *firstly* on the ground that the impugned transaction had taken place through INB[3]wherein OTPs were received by the petitioner, and *secondly* on the ground that he accessed a link forwarded by an unknown person that led to the deduction of funds from his bank account.

6. Aggrieved by the impugned rejection letter dated 26.07.2021, the distraught petitioner again approached the respondent no.1/RBI by way of complaints dated 06.08.2021 and 31.08.2021, seeking re-investigation in the matter and expeditious disposal of his complaint,

[2] Centralized Public Grievance Redress and Monitoring System
[3] Internet Banking

in which he specifically alleged that he did not share any One Time Password **['OTP']** with the said caller at any point in time.

7. Pursuant thereof, the BO, New Delhi-II passed an order dated 20.10.2021, the relevant portion of which is reproduced hereinunder:

> "2……It seems that the customer is a victim of vishing, he got defrauded when clicked an unknown link (copy of FIR attached). though the transaction are secured with 2 FA that is OTP, It has been observed that the customer is familiar with the INB application and POS transactions as he has been doing it earlier.
> The transaction of Rs. 160,000/- was made to One97 communication which is not under BO purview...
> Sbi was advised to pay 1/3 of the amount of the disputed amount of Rs 100,000 /- i.e.33340/-
> 3. As the grievance raised by the complainant has been resolved by the bank or the concerned subsidiary of a bank with the intervention of the Banking Ombudsman, accordingly your complaint was closed under Clause 11(3)(a) of BOS-2006 as 'settled by the bank'.
> Please note that complaints closed under the aforesaid Clause are not appealable before the Appellate Authority in Reserve Bank of India. Details of BOS-2006 are available at our website www.rbi.org.in/commonman.
> 4. You may note that despite the rejection of your complaint by the Banking Ombudsman, as aforesaid you are at liberty to approach a Civil Court of competent jurisdiction or such other authority in accordance with law for the redressal of your grievance.
> 5. This has been issued under the orders of the Banking Ombudsman"

8. Resultantly, upon the advice of the 'BO', one-third of the disputed amount i.e., Rs. 33,334/- was in fact credited by the SBI, Greater Noida branch, in the account of the petitioner on 06.10.2021 and the complaint was closed. The petitioner is aggrieved insofar as the unauthorised withdrawals in the sum of Rs. 2,27,000/- have still not been restored by the SBI to his bank account as yet, despite the guidelines issued by the RBI *vide* circular titled "Customer Protection

– Limiting Liability of Customers in Unauthorised Electronic Banking Transactions" dated 6th July, 2017, that creates a framework for reversal of erroneous debits arising from fraudulent or other transactions. Hence, the present petition.

9. It is pertinent to mention here that while the respondent No.1/RBI has chosen not to file any reply, respondents No. 2 and 3 i.e. the SBI were granted sufficient opportunities to file a reply/counter-affidavit *vide* order dated 22.12.2022, and last opportunity to file the reply/counter-affidavit was granted *vide* order dated 30.10.2023 within four weeks from that day, and as the same was not filed, the right to file reply/counter-affidavit was closed by this Court *vide* order dated 03.09.2024.

ARGUMENTS ADVANCED AT THE BAR:

10. Learned counsel for the petitioner has urged that the SBI should devise a mechanism more robust than the 'secured socket layer connection' so as to identify fraud risk by way of vishing, phishing, trojans, session hijacking, key logger, etc., as well as the location behaviour of the hijackers/fraudsters and effectively protect the interests of the account holders. Pertinently, strong reliance has been placed by the learned counsel on clause (6) of the RBI circular dated 06.07.2017 to show the petitioner's entitlement to zero liability in the unauthorised transactions dated 18.04.2021. Reliance has been placed on the decision in the case of **Tony Enterprises v. Reserve Bank of India**[4] to substantiate his plea that the SBI thereafter, will have an

[4] W.P(C) No. 28823/2017 decided on 11.10.2019

appropriate remedy by way of filing a civil suit for claiming the loss suffered in the unauthorised transactions and to recover it from the person responsible.

11. Learned counsel for the respondent no.1/RBI challenged the maintainability of the present petition *qua* the RBI in as much as neither any cause of action nor any relief as against the RBI has been pleaded in the present petition. On merits, it is submitted that though the petitioner was indeed held to be a victim of 'vishing' by the 'BO', his case falls under clause (7)(b)(i) of the RBI circular dated 06.07.2017 as negligence on the part of the petitioner cannot be ruled out, considering that the disputed transactions were 2FA (Two Factor Authenticated) transactions i.e., they were carried out using the INB credentials and an OTP, thereby suggesting that the petitioner must have shared the OTP with the unknown caller. Alternatively, it is submitted that the BO is willing to reconsider and decide the present matter afresh if so directed by this Court.

12. Learned counsel for the respondent Nos. 2 and 3/SBI have challenged the maintainability of the present petition for lack of territorial jurisdiction. On merits, it is contended that the present matter involves disputed questions of facts pertaining to the manner in which the alleged unauthorised transaction took place, which cannot be determined in the present proceedings. In tow with the other respondent, it is contended that the SBI cannot be held liable for the loss suffered by the petitioner due to his own negligence insofar as he accessed the unknown link from his mobile phone. Accordingly, it is submitted that the case of the petitioner is covered under clause

(7)(b)(i) and not clause (6) of the RBI circular dated 06.07.2017. Reliance has been placed on the decisions in **Punjab National Bank v. Shri Sankar Mukherjee** and **ICICI Bank Limited v. Mr. Uma Shankar Sivasubraminaian.**

ANALYSIS & DECISION:

13. I have given my thoughtful consideration to the submissions advanced by the learned counsels for the parties at the Bar. I have also perused the relevant record of the case. I have also gone through the written submissions which have been filed on behalf of the respondent No.1/RBI as well as respondents No.2 and 3, besides the petitioner.

14. **First things first,** the challenge to the territorial jurisdiction of this Court to entertain and adjudicate upon the present writ petition by the respondents No. 2 and 3 is not sustainable in law. Although, the transaction took place involving the SBI branch at Greater Noida, however, the decision by the 'BO' i.e. the respondent No.1 has been made at Delhi and the SBI has its Regional Office at Delhi as well. Moreover, the amount in question had been remitted to financial concerns at Delhi. Therefore, it is but clear that not only the respondents are carrying on their work from Delhi but even a substantial part of the cause of action had arisen at Delhi.

15. That being the case, the broad facts of the matter are not in dispute. Evidently, the petitioner was a victim of 'phishing' as well 'vishing'. He got duped when he clicked on an unknown *link* sent on

his mobile number 98XXXXXX78[5] from mobile number 9470062057. The petitioner was tricked into clicking on the said link sent through SMS accompanied with a call to the effect that if he would not click on the link, his SMS services would be closed. The petitioner acknowledges that he received 'OTPs' on his mobile number, and thereafter, an SMS was received communicating a withdrawal of Rs. 1,00,000/- from his bank account, and while he was in the process of making a complaint to the SBI Customer Care *vide* reference No. 1800111109, a sum of Rs. 1,60,000/- was further withdrawn from his bank account as per another SMS received on his mobile.

16. In the said backdrop, it is significant to note that the petitioner **categorically submits that he had never shared the OTPs**, of which fact there is no specific denial by the respondents. In other words, although he did receive the OTPs, but the same were not shared with a third party. As the phishing/vishing phenomena in cyber attacks implies, the moment the link was clicked, the mobile phone of the petitioner got hacked and the OTPs passed on to the cyber fraudster, who then managed to withdraw aforesaid amount. At this juncture, it is pertinent to mention that respondent No.1 in its written submissions elaborates that based on the documentary evidence produced by the SBI, the 'BO' observed that INB was successfully logged in at 17:09:55 hours and 17:28:03 hours on 18.04.2021 and the OTPs were delivered to the petitioner's registered mobile No. 98XXXXXX78 on

[5] The personal mobile number of the petitioner is concealed so as to protect the privacy of the petitioner herein

three occasions at 17:10:18, 17:28:15 and 17:29:42 on 18.04.2021 for approval of transaction of Rs. 10/-, Rs. 1,00,000/- and Rs.1,00,000/- respectively which were followed by transaction acknowledgments through SMS. The said documentary evidence has not been placed on the record and deliberately kept away.

17. The question that arises for consideration is: whether the victim i.e., the petitioner was negligent so as to fall prey to the scamsters ? Indeed, the answer is in the affirmative. But then anyone, regardless of age, education, or experience, can fall victim to the sophisticated cyber-attacks prevalent today. At the same time, it is also an admitted fact that the petitioner promptly dialled SBI Customer Care Service and lodged a report, but unfortunately, the transaction had already been processed.

18. It is an admitted fact that the petitioner lodged a report on the same day i.e. 18.04.2021 at 5.50 p.m. on the Online Portal of Cyber Crime and then subsequently with the bank on 19.04.2021 and ultimately with the Police on 20.04.2021. The respondents take shelter behind the RBI Circular dated **06.07.2017** titled "**Customer Protection– Limiting Liability of Customers in Unauthorised Electronic Banking Transactions**", the relevant provisions of which are extracted below:

> **Limited Liability of a Customer**
> **(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.

(b) Limited Liability of a Customer

7. A customer shall be liable for the loss occurring due to unauthorised transactions in the following cases:

(i). In cases where the loss is due to negligence by a customer, such as where he has shared the payment credentials, the customer will bear the entire loss until he reports the unauthorised transaction to the bank. Any loss occurring after the reporting of the unauthorised transaction shall be borne by the bank.

(ii) In cases where the responsibility for the unauthorised electronic banking transaction lies neither with the bank nor with the customer, but lies elsewhere in the system and when there is a delay (of four to seven working days after receiving the communication from the bank) on the part of the customer in notifying the bank of such a transaction, the per transaction liability of the customer shall be limited to the transaction value or the amount mentioned in Table 1, whichever is lower.

Table 1

Maximum Liability of a Customer under paragraph 7 (ii)

Type of Account	Maximum liability (₹)
• BSBD Accounts	5,000
• All other SB accounts • Pre-paid Payment Instruments and Gift Cards • Current/ Cash Credit/ Overdraft Accounts of MSMEs • Current Accounts/ Cash Credit/ Overdraft Accounts of Individuals with annual average balance (during 365 days preceding the incidence of fraud)/ limit up to Rs.25 lakh • Credit cards with limit up to Rs.5 lakh	10,000
• All other Current/ Cash Credit/ Overdraft Accounts • Credit cards with limit above Rs.5 lakh	25,000

Further, if the delay in reporting is beyond seven working days, the customer liability shall be determined as per the bank's Board approved policy. Banks shall provide the details of their policy in regard to customers' liability formulated in pursuance of these directions at the time of opening the accounts. Banks shall also display their approved policy in public domain for wider

dissemination. The existing customers must also be individually informed about the bank's policy.

Burden of Proof

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

19. A careful perusal of the aforesaid instructions would show that the burden of proving the customer's liability in case of unauthorized electronic banking, lies upon the bank. The respondents invokes clause (7) but then one has to understand whether the loss occurred due to negligence by the customer? The record shows that he had never shared the payment credentials, which fact is fortified from the written submissions filed by the respondents that the OTPs were not shared by the petitioner as such. It is merely upon clicking on a link received on his mobile phone after he was duped into believing that his SMS services would be blocked, that the said unauthorised transactions took place.

20. While there is no exact definition of the term "phishing" or "vishing", Phishing is a type of cybercrime where attackers trick victims into revealing sensitive information while vishing is a type of scam where the fraudsters use phone calls to tricks victims into revealing sensitive financial information. At the cost of repetition, in the instant case, there is nothing to suggest that the petitioner shared the sensitive financial information, rather this is a case where the OTPs received on the mobile phone of the petitioner automatically got transmitted to the cyber fraudsters who thereby were able to withdraw the amount from the account of the petitioner.

21. In my view, the petitioner was a 'victim' of cyber fraud and he cannot be said to be 'negligent' in any manner under the notions of the civil law or for that matter under the criminal law. Negligence implies "the duty to take care" that would be expected from a person of ordinary prudence. The negligent act on the part of the customer should be such which is gross, utterly reckless and unconscionable. In the present case, the petitioner had taken care not to share the OTPs, in fact he had no occasion do so, and if that is the case, it would imply that even the most hyped 2 Factor Authentication ["2FA"] was breached as the same was not secure, which is directly attributable to deficiency in service provided by the respondent no. 2 & 3 SBI.

22. Be that as it may, what *turns the table* against the respondents No. 2 and 3 is that in their written submissions and during the course of trial, they acknowledged that on internal inquiries conducted by them, they immediately were able to track that Rs. 1,00,000/- had been credited in an account maintained with IDFC Bank whereas Rs. 1,60,000/- had been credited to One97 Communications Limited **['OCL'].** Respondents No. 2 and 3 fail to provide a satisfactory explanation for their inability to initiate a chargeback, reclaim, or block the amount despite the petitioner's prompt complaint to SBI Customer Care Service on the same day, within a few minutes from the transaction. Instead, they offer a weak justification, claiming that the relevant rules only apply to commercial banks, regional rural banks, and scheduled primary cooperative banks, and thus do not cover OCL.

23. The said defence is not fathomable and is belied from the subsequent RBI Circular dated **04.01.2019** vide No. DPSS.CO.PD.No.1417/02.14.006/2018-19 titled "**Customer Protection– Limiting Liability of Customers in Unauthorised Electronic Payment Transactions in Prepaid Payment Instruments (PPIs) issued by Authorised Non-Banks**", the relevant provision of which reads as under:

Limited liability of a customer

6. A customer's liability arising out of an unauthorised payment transaction will be limited to:

Customer liability in case of unauthorised electronic payment transactions through a PPI

S. No.	Particulars	Maximum Liability of Customer
(a)	Contributory fraud / negligence / deficiency on the part of the PPI issuer, including PPI-MTS issuer (irrespective of whether or not the transaction is reported by the customer)	Zero
(b)	Third party breach where the deficiency lies neither with the PPI issuer nor with the customer but lies elsewhere in the system, and the customer notifies the PPI issuer regarding the unauthorised payment transaction. The per transaction customer liability in such cases will depend on the number of days lapsed between the receipt of transaction communication by the customer from the PPI issuer and the reporting of unauthorised transaction by the customer to the PPI issuer -	
	i. Within three days#	Zero
	ii. Within four to seven days#	Transaction value or ₹10,000/- per transaction, whichever is lower
	iii. Beyond seven days#	As per the Board approved policy of the PPI issuer
(c)	In cases where the loss is due to negligence by a customer, such as where he / she has shared the payment credentials, the customer will bear the entire loss until he / she reports the unauthorised transaction to the PPI issuer. Any loss occurring after the reporting of the unauthorised transaction shall be borne by the PPI issuer.	
(d)	PPI issuers may also, at their discretion, decide to waive off any customer liability in case of unauthorised electronic payment transactions even in cases of customer negligence.	

 # The number of days mentioned above shall be counted excluding the date of receiving the communication from the PPI issuer.

24. As for the case law referred to by the learned counsels for the respondents, the decision in the case of **Raghabendra Nath Sen v. Punjab National Bank**[6] was one where the ATM[7] had been used by the customer, and therefore, it was held that there was no possibility of

[6] [I(2015) CPJ 254]
[7] Automatic Teller Machine

anyone withdrawing any cash through ATM even if one is able to clone the ATM/debit card issued to the customer. **State Bank of India v. K.K. Bhalla**[8] was a case where it was held that ATM-cum-debit card and PIN number allotted to the customers are to be kept in their safe custody and the petitioner bank has no control over the same and once the ATM-cum-debit card is known to the customer and he uses the same, which is not shared with the bank, there is no deficiency in services on the part of the petitioner bank. The decision in the case of **Punjab National Bank v. Shri Sankar Mukherjee**[9] was one where the petitioner had apparently shared the payment credentials that enabled the fraudster to withdraw the money from his account, which case was squarely covered by Clause (7)(i) of the aforesaid circular issued by the RBI.

25. In summary, the aforesaid decisions do not help the respondents No. 2 and 3 in any manner. On the other hand **Tony Enterprises v. Reserve Bank of India**[10] was a case where the Kerala High Court dealt with two cases wherein the customer's mobile had been dysfunctional since a duplicate SIM card had been issued by the service provider to a fraudster impersonating as the real mobile holder, which enabled the fraudster to withdraw a huge amount from the bank account of the customer through on line transfer. It was in the said backdrop, it was observed as under:

> "**13.** 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

[8] [II (2011) CPJ 106 (NC)]
[9] MAT 2483 of 2023
[10] AIR OnLine 2019 KER 674

> 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."

26. It was further held that:

> "**20.** Thus, it is clear that the bank cannot claim any amount from the customer when a transaction is shown to be a 'disputed transaction'. The bank can recover from the customers only when it can unequivocally prove that the customer was responsible for such transaction, independently through the civil court. The RBI guidelines is a clear mandate to exonerate a customer in such 'disputed transaction'. RBI circular presumes the innocence of the customer in such given circumstances. However, this innocence can be controverted. The onus falls on the bank to prove otherwise."

27. Reverting back to the instant matter, it is undeniable that customer care services play a crucial role in supporting bank customers with various concerns, including suspicious account activity, compromised debit/credit card security, and issues concerning online banking services. The term 'deficiency' in service in terms of the meaning assigned vide Clause (6)(a) of the aforesaid RBI instructions, in plain dictionary meaning would imply

insufficiency, shortage, dearth, deficit, shortfall and so on. Incidentally, the term 'deficiency' is defined under Section 2(11) of the Consumer Protection Act, 2019 to mean "*any fault, imperfection or shortcoming or inadequacy in the quality, nature and manner of performance which is required to be maintained by or under any law for the time being in force or has been undertaken to be performed by a person in pursuance of a contract or otherwise in relation to any service and includes (i) any act of negligence or omission or commission by such person which causes loss or injury to the consumer or (ii) deliberate withholding of relevant information by such person to the consumer.*"

28. In the instant case, respondents No. 2 and 3 demonstrated a glaring service deficiency. Despite prompt intimation from the petitioner about the account breach, they showed no urgency. Respondents No. 2 and 3 failed to exercise due care, neglecting their duty to act swiftly upon notification of the fraudulent withdrawal. Consequently, they took no steps towards chargeback, retrieval, or freezing the suspicious accounts maintained with IDFC Bank and One97 Communication.

29. The aforesaid view is also fortified from the RBI's **Master Direction on Digital Payment Security Controls** dated **18.02.2021**, vide RBI/2020-21/74 DoS.CO.CSITE.SEC.No.1852/31.01.015/2020-21, which lays down certain guidelines that apply to the following Regulated Entities **['REs']:**

a) Scheduled Commercial Banks (excluding Regional Rural Banks);
b) Small Finance Banks;
c) Payments Banks; and

d) Credit card issuing NBFCs.

30. The RBI Master Directions further lays down the guidelines for governance and management of security risks, as under:

> **4.** REs shall formulate a policy for digital payment products and services with the approval of their Board. The contours of the policy, while discussing the parameters of any "new product" including its alignment with the overall business strategy and inherent risk of the product, risk management/ mitigation measures, compliance with regulatory instructions, customer experience, etc., should explicitly discuss about payment security requirements from Functionality, Security and Performance (FSP) angles such as:
>
> a) Necessary controls to protect the confidentiality of customer data and integrity of data and processes associated with the digital product/ services offered;
>
> b) Availability of requisite infrastructure e.g. human resources, technology, etc. with necessary back up;
>
> c) Assurance that the payment product is built in a secure manner offering robust performance ensuring safety, consistency and rolled out after necessary testing for achieving desired FSP;
>
> d) Capacity building and expansion with scalability (to meet the growth for efficient transaction processing);
>
> e) Minimal customer service disruption with high availability of systems/ channels (to have minimal technical declines);
>
> f) **Efficient and effective dispute resolution mechanism and handling of customer grievance; and**
>
> g) **Adequate and appropriate review mechanism followed by swift corrective action**, in case any one of the above requirements is hampered or having high potential to get hampered. **{bold portions emphasized}**

31. The aforesaid Master guidelines under the title "Customer Protection, Awareness and Grievance Redressal Mechanism" *inter alia vide* Regulation (50) provides as under:

> **50.** REs should provide a mechanism on their mobile and internet banking application for their customers to, with necessary authentication, identify/ mark a transaction as fraudulent for seamless and immediate notification to his RE. **On such**

> **notification by the customer, the REs may endeavour to build the capability for seamless/ instant reporting of fraudulent transactions to the corresponding beneficiary/ counterparty's RE; vice-versa have mechanism to receive such fraudulent transactions reported from other REs.** The objective of this mechanism is to accelerate early detection and enable the banking/ payment system to trace the transaction trail and mitigate the loss to the defrauded customer at the earliest possible time.
>
> **{bold portions emphasized}**

32. In the light of the aforesaid regulations, it is evident that the security protocols such as '2FA' or OTP verification had been breached by a simple 'malware' deployed by the cyber fraudsters. Evidently, the online banking service of the petitioner was linked with his mobile number, which was being used to authenticate his banking transactions, and the security apparatus of the respondent Bank failed to detect any unusual logging activity from a different Internet Protocol Address that was being used by the fraudsters. It has to be presumed that it is on account of the failure on the part of the bank to put in place a system which prevents such withdrawals, that the petitioner suffered monetary losses.

33. Lastly, it is well established under the Common Law, that funds in a bank account belong to the bank, but the bank acts as an agent for the principal (the customer). Consequently, the bank cannot refuse to process an online transfer if it appears to be authorized by the customer, however, upon detecting fraud, the bank has an implied duty to exercise reasonable care and take prompt action. Unhesitatingly, there was patent deficiency in services on the part of the bank, inasmuch as the response of the bank was lukewarm, defective, and not prompt. The respondent No. 2 i.e., SBI failed to

take immediate measures to take up the issue with the other REs to whom the online payment had been remitted.

34. In view of the foregoing discussion, this Court finds that the Banking Ombudsman (BO) has failed to judiciously consider the entire gamut of the controversy. The 'BO' overlooked the aforesaid key aspects of the matter and completely misdirected itself in law. Consequently, the impugned order dated 20.10.2021 is legally unsustainable. In view of the respondent No.2 and 3/SBI's violations of the aforesaid mandatory Master Guidelines formulated by the respondent No.1/RBI, the maintainability of the instant writ is beyond any challenge. It must be indicated that the aforesaid guidelines are by and large measures that the REs or the banks have to undertake, and the said guidelines do not restrict an affected party to take legal recourse for redressal of their grievances. The transactions in question would resultantly fall within the sweep of "zero liability" as referred to in the aforesaid RBI Circulars. Therefore, respondents No. 2 and 3/SBI are liable to compensate the petitioner for the incurred loss, along with interest, and pay token compensation.

RELIEF:

35. In view of the aforesaid discussion the present writ petition is allowed and the impugned order dated 20.10.2021 passed by the 'BO' is hereby set aside. A writ of *mandamus* is issued against the respondents No. 2 and 3/ State Bank of India, to make payment of Rs. 2,60,000/- to the petitioner with interest @ 9% per annum from the date the fraud was reported i.e. 18.04.2021 within four weeks from today along with costs for legal proceedings, which is quantified as

Rs.25,000/-. The amount, if any, paid to the credit of the bank account of the petitioner, shall be adjusted towards the outstanding interest.

36. The present writ petition stands disposed of accordingly.

DHARMESH SHARMA, J.

NOVEMBER 18, 2024
Sadiq