IN THE HIGH COURT OF JUDICATURE AT BOMBAY

ORDINARY ORIGINAL CIVIL JURISDICTION

WRIT PETITION NO. 2791 OF 2023

PNP Polytex Private Limited,
a Company incorporated under the Companies Act, having its office at A-601-607, Mangal Aarambh, Kora Kendra, Borivali (W), Mumbai-92. .. Petitioner

Versus

1) Reserve Bank of India, through its Regional Director, Main Building, Shahid Bhagat Singh Road, Kala Ghoda, Fort, Mumbai 400001.
2) Bank of Baroda, Through its General Manager, Baroda Bhavan, RC Dutt Road, Alkapuri, Baroda 390007.
3) Bank of Baroda, through its Regional Manager, Baroda House, 5th floor, Behind Deewan Shopping Centre 2, S.V. Road, Jogeshwari (W) Mumbai 400102.
4) Bank of Baroda, through Branch Manager, Jaya Talkies Bldg, SV Road, Borivali (W), Mumbai 4000092.
5) Vodafone Idea Limited, through General Manager, Birla Centurion, Century Mills Compound, Worli, Mumbai 400032.
6) Union of India, Through Secretary Telecommunications, Dept of Telecommunications, Sanchar Bhavan, 20 Ashoka Road, New Delhi 110001.
7) Telecom Regulatory Authority of India, Through Chairman, Mahanagar Doorsanchar Bhavan, New Delhi.
8) The Superintendent of Police, Borivali West Police Station, Mumbai. .. Respondents

...

Ms. Shilpi Jain with Mr. Sumit Raghani i/b Agrud Partners for the petitioner.
Mr.Prasad Shenoy with Ms. Aditi Phatak, Ms. Parichar Zaiwalla and Ms.Ishita Desai i/b BLAC Co. for respondent no.1 – RBI.
Ms.Prashansa Agrawal with Ms. Kirti Singh i/b Nahush Shah Legal for respondent no.4 (Bank of Baroda)
Mr.Mustafa Doctor, Sr. Advocate with Ms. Sneha Jaisingh, Mr.Akshay Ayush & Ms.Asha Anandkumar i/b Bharucha & Partners for respondent no.5.
Mr.Ashok R. Varma with Mr.Vinit Jain and Mr. Gaurav Mhatre for Union of India – respondent no.6.

CORAM : BHARATI DANGRE &
MANJUSHA DESHPANDE, JJ
RESERVED ON: 18th FEBRUARY, 2026
PRONOUNCED ON : 28th APRIL, 2026

JUDGMENT :- (Per Bharati Dangre, J)

1 PNP Polytex Private Limited, a Company incorporated under the Companies Act, and engaged in Import and Trade in various products ranging from luggage, furniture, Nylon Yarn, Ventilators etc, suffered a loss of Rs.1.24 crores, as the account maintained by the Company with Bank of Baroda (referred to as “the Bank”) with whom it was maintaining multiple current accounts with a common customer ID was debited on 13/1/2020, by transferring the amount to 7 different bank accounts opened in various cities. The aforesaid amount being diverted from the two cash credit account, it took immediate steps by forwarding an intimation to the Bank and instructing them to debit freeze all their accounts maintained with the Bank. The petitioner also forwarded a handwritten complaint

to Borivali Police Station which was converted into CR No. 20/2020 with regards to the online fraud of Rs.1.24 crores. The petitioner also lodged a complaint with the National Cyber Crime through a portal maintained for reporting of online frauds.

The claim in the petition is for refund of the amount by the Bank, as it suffered huge loss on account of the operation of a gang of fraudsters who carefully planned and executed the online fraud.

The petition before us therefore, seek the following reliefs.

> (a) this Hon'ble Court be pleased to issue writ of mandamus or a writ in the nature of mandamus or any other appropriate writ, order or direction under Article 226 of the Constitution of India, ordering and directing the respondent no.1, its subordinate servants and agents to unconditionally implement and enforce the RBI Master Circular dated 6th July, 2017
>
> (b) this Hon'ble Court be pleased to issue a writ of mandamus or in the nature of the mandamus or any other appropriate writ, order or direction under Article 226 of the Constitution of India, ordering and directing the respondent no.2 to 4, its subordinate servants and agents to declare that the petitioner has zero liability towards the unauthorised debit which took place in their bank account amounting to Rs.1.24 crores
>
> (c) this Hon'ble Court be please to issue a writ of mandamus or in the nature of the mandamus or any other appropriate writ, order or direction under Article 226 of the Constitution of India, ordering and directing the respondent nos.2 to 4, its subordinate servants and agents to immediately refund Rs.1.24 crores along with the interest charged at the rate of 14.4% till the date of passing the order.
>
> (c-1) this Hon'ble Court be pleased to issue a writ of mandamus or in the nature of the mandamus or any other appropriate writ, order or direction under Article 226 of the Constitution of India, ordering and directing the respondent no.1 – RBI, its subordinate servants and agents to withdraw the impugned email dated 2nd February, 2023 (being Exhibit 'Y') whereby it had rejected the petitioner's claim with regards to unauthorised;

2. We have heard learned counsel Ms. Shilpi Jain for the Petitioner Company.

The petition has impleaded Bank of Baroda through its General Manager/Regional Manager and Branch Manager as respondent nos.2, 3 and 4 respectively. Ms. Prashansa Agarwal has marked her appearance for Bank of Baroda. The Reserve Bank of India which is impleaded as respondent no.1 is represented by Mr. Prasad Shenoy. Respondent no.5 Vodafone Idea Limited is represented by Senior Counsel Mr. Mustafa Doctor. The learned counsel Mr. Ashok Verma has marked his appearance for respondent no.6 Union of India.

Upon the pleadings being completed in the petition, as the contested respondents have filed their affidavits in reply and rejoinder affidavits being filed, at the request of the learned counsel representing the parties, we have taken up the petition for final hearing at the stage of admission. Hence. Rule. Rule is made returnable forthwith.

3. It is the case of the petitioner that as a Company it was maintaining multiple current accounts with the respondent no.4 Bank with a common customer ID and it also availed the online banking facility and had transacted on numerous occasions availing the facility. The petitioner is conscious of the fact that to initiate any online transaction, the customer has to login through Banking Home page by inserting exclusive Customer ID and password. Upon this step being completed, One Time Password (OTP) is received on the registered mobile number of

the customer and on submission of this password, customer's online transaction is allowed to be completed.

According to the petitioner, in order to safeguard against any misuse of the online account, the petitioner company had designated a separate registered number only for receiving OTP pertaining to online transaction and the mobile with the said number was always kept in locker under supervision.

4. On 13/1/2020 at around 10.00 a.m, when one of the employees of the Petition Company tried to log in to the Current Credit Bank Account in respondent no.4 Bank from regular corporate ID, it gave a message of invalid password. Thereafter, the employee logged in from its alternate corporate ID, which had only viewing access.

On this indulgence, he was shocked to notice multiple online transactions from the account, debiting an amount of Rs.1.24 crores (Rupees One Crore Twenty Four lakhs) from the two cash credit accounts with No. 0380-050000-0070 and 0390-050000-0106 of the Company. The amount of Rs.1,24,00,000/- was debited through 14 transactions in the two accounts on two dates i.e. 12/1/2020 and 13/1/2020. The bank statement reveal that the amount was transferred to seven different accounts.

Immediately, upon becoming aware of the aforesaid unauthorised transactions, on the very same day i.e. 13/1/2020, the attention of the Bank was invited through a communication in writing about the fraudulent transaction in

its Current Credit Accounts, with a request to freeze all debit transactions in all cash credit and current accounts held in the Bank till further instructions, and start investigation for bringing the amount back into the account of the Company. On the very same day, an FIR is also lodged, copy of which is annexed along with the petition.

5. It is the case of the petitioner that the Company has been duped by unauthorised fraudulent transactions, which was carried out in two out of the seven accounts maintained by the Company with Bank of Baroda. On further details being secured, it is noticed that 18 different bank accounts were opened at multiple locations including West Bengal, Mathura, Gwalior and the money was transmitted into these accounts.

In order to apprise the Court of the further steps that have been taken in this regard, the petition contain a statement that, between 13/1/2020 and 17/1/2020, the Mathura police arrested four individuals involved in the racket and they were remanded to Mumbai for investigation. A specific statement is also made that there is a big racket was involved in the online fraud, and as a part of it, the petitioner has suffered a loss of Rs.1.24 crores, which amount was transferred into 18 accounts. The petitioner also intimated the banks in which the funds were transferred, which included HDFC Bank, ICICI Bank, Bank of Baroda and Yes Bank, with a request to freeze the respective accounts. However, when the request reached the Bank, a large chunk of money was already withdrawn, but the

petitioner was able to freeze some accounts and prevented a sum of Rs.47,87,750/- being withdrawn.

6. By collating the information in regards to the fraudulent transactions, the petition contain a statement that the accounts were debited and the Company was a victim of online fraud, which occurred due to SIM swapping. The petition contain the following statements in this regards :-

> 13. On further investigation, Petitioner found that the online fraud had taken place by way of SIM swapping. To the shock of the Petitioner, its SIM card no. 89910271001159369960 used for its registered mobile no. 9223391091 was blocked and a new SIM card no. 89910271001127988099 for the above said registered mobile number was procured by the fraudsters for the unauthorized online bank transfer.
>
> 14. On 12th January 2020, which was Sunday, fraudsters hacked Petitioner's Bank Account and started adding beneficiaries in the Bank Account. On Monday morning, i.e, 13th January 2020, fraudsters started initiating online fraudulent transfers by using the duplicate SIM card. Since the Petitioner's SIM card was blocked on Sunday, Petitioner did not get any intimation for the same. All the intimations and the OTP's were diverted to the duplicate SIM card.
>
> 15. It is submitted that SIM swapping is the theft wherein fraudster procures a duplicate SIM card by providing fake identity cards to the mobile service provider against the registered mobile number of the targeted bank customer. Thereafter, the duplicate SIM card is used to procure one time passwords (OTP) generated through the banking system to operate customer person's bank account. SIM Swapping is identity theft. Identity theft in cyberspace means fraudulent means of using another person's name and personal details in order to gain the benefit of financial advantage. The person, whose identity is the subject of the theft would suffer loss."

7. The petitioner addressed various communications to the service provider, respondent no.5 as to how a new SIM could be provided without document verification and the respondent no.5 through its e-mail dated 17/1/2020 confirmed that the SIM replacement was done without the company's consent and a following statement is found in the said letter :-

> "I have checked the details in regards to your inquiry and found the following :
> As per our telephonic conversation, SIM replacement is done without your consent."

It is therefore, the pleaded case of the petitioner that the service provider, Vodafone Idea Limited, has replaced the SIM without documentation or authorization and this is completely against public policy as well as the guidelines issued by the Company itself, as the SIM was replaced on the basis of the call from a fraudster.

8. The Petitioner has placed heavy reliance on the Master Circular dated 6/7/2017 issued by the Respondent no.1, Reserve Bank of India (RBI), with the intention of protecting the customers of the Bank in unauthorised electronic banking transactions and according to the petitioner, the said Circular has set out the rights and obligations of the customers in case of unauthorised transactions in specific situation. As per the said circular, if unauthorised transaction has taken place, without negligence of the customer, and the same is intimated to the Bank within three days, then the customer will bear zero liability towards unauthorised transaction and in such situation, when the bank is intimated of such a transaction, which is not authorised by the customer, the amount under the transaction shall be credited to the customer's account within ten days.

Taking benefit of the said circular, the petition plead that the Reserve Bank of India had directed all the Banks to revise their customer protection policy, to cover aspects of customer

awareness on the risk and responsibility involved in the electronic banking transaction and impose zero liability on the customer, who is not at fault. Relying upon the said Circular, it is the case pleaded by the petitioner that it was duped of a huge sum of Rs.1.24 crores, but only sum of Rs.47,81,750/- was frozen and according to the petitioner, there was no negligence which could be attributed to it, as the petitioner was diligent while using the online services and despite this, it has been defrauded, for which in no case, the petitioner can take the blame.

9. As per the Petitioner, the policy for protection of the customer contained in the circular dated 6/7/2017 issued by the Reserve Bank of India protect the customer who is not guilty of any negligence or contributory negligence, the petitioner filed a complaint and requested for an action to be taken. A complaint was also filed to the Ombudsman under the Banking Ombudsmen Scheme 2006 and the complaint was registered as complaint no. 201920013013933.

During the pendency of the present petition, the petitioner received a response on 2/2/2023 from the Reserve Bank of India, informing that the complaint is rejected, as it is informed that there are multiple security features which have been cleared and fraud cannot happen without compromise of the account credentials by the customer and therefore, based on the bank submission and the documents, it is recorded that there is no system lapse on part of the Bank and no deficiency

in banking service and therefore, no relief can be provided to the petitioner.

The petition also raise a challenge to this rejection.

10. The petitioner is aggrieved by non-redressal of its grievance by RBI as well as Bank of Baroda, with which it shared a long drawn relationship as it had maintained numerous accounts in the Bank, since the year 2007. According to the petitioner, Reserve Bank of India has also failed to discharge its obligation of protecting the customer and it merely accepted the stand of the Bank of Baroda, that there was no shortcoming in the banking services but it remained unmindful of its own circular, where the burden to prove the negligence of the customer is on the Bank and since the Bank of Baroda had failed to prove the same, the petitioner is entitled for the benefit of the Circular providing for zero liability. According to the petitioner, the fraudulent transactions were possible due to SIM swapping and since some third party was responsible for fraud and with no contribution in negligence at the petitioner's end and moreso the Bank had failed to establish that the petitioner was at fault, the petitioner is entitled for benefit of the said Circular by reversal of the amount which is debited from its accounts.

11. The learned counsel, Ms.Shilpi Jain would lay emphasis upon the circular issued by the RBI and she would submit that the RBI involved itself and took necessary steps to prevent loss to the customers by formulating Customer Protection Policy

(unauthorised electronic banking transactions) and according to her, the circular was intended to confer protection on the customers, who have grievance(s) pertaining to unauthorised transactions and on one hand, when the RBI was encouraging online banking transaction, and provide a buffer to the customers who adopt themselves to the online banking transactions but fall prey to some fraudulent unauthorised transactions, the policy comes into play.

Highlighting that the objective of the policy is to make customers more confident against the risks arising out of unauthorised debits to their account(s) owing to customer negligence/bank negligence/banking system fraud/third party breaches, the policy also aim to define the right and obligations of the customer, in case of unauthorised transaction in specified scenarios by use of electronic banking and it define the maximum customer liability. According to her, while formulating the said policy, the Reserve Bank clearly contemplated grant of protection to the customer against unauthorised transaction, but according to her, neither the RBI nor Bank of Baroda has averred to the specific objective underlying the said policy, and when the petitioner had fallen prey to a fraudulent transaction and has been duped of a sum of Rs.1.24 crores, without the Bank of Baroda proving any negligence/contributory negligence, the RBI had failed to redress the grievance of the petitioner, who was all the while diligent in availing the online services.

According to Ms. Jain, the present case is the case of Cyber Crime and SIM swapping, where the fraudster had secured duplicate SIM and utilised it to unlawfully transfer the funds from the petitioner's account and this is evidently clear from the affidavit of the service provider Vodafone Idea Ltd, respondent no.5, who do not dispute that a request was received by it to replace the SIM and the request was granted. She also blame the service provider in permitting replacement of the SIM merely on a telephonic request without ascertaining the veracity of such a request.

Thus, it is the submission advanced on behalf of the petitioner that in terms of the policy of the RBI, since no negligence is attributed to the petitioner, who had fallen prey to a cyber crime and has lost a huge sum of money, it must be compensated by reversing the entry of the aforesaid amount barring the amount which has been secured and which must also be refunded to the petitioner.

12. The petition is strongly contested by Bank of Baroda, the Bank offering banking services to the petitioner company. The Chief Manager and Authorised Signatory of Bank of Baroda, in its affidavit, state that the Bank has multiple security layers for any successful online transaction and it has set out the procedure which is followed in the following words :-

> "It is pertinent to note here that the respondent no.4 has multiple security layers for any successful online transaction to take place. The first and foremost being the unique Login User ID which is distinct for each customer and the password which is set by the customer himself and can be changed by the customer only. Moreover, if the system of the Bank suspects that a particular customer is logging in from a new system, then in that event an

OTP is sent to the registered mobile number of the customer to validate and authenticate the account. After logging in, the details of the beneficiary are required to be added for fund transfer, which is immediately confirmed by the tracker ID sent to the registered mobile number of the customer. Pursuant thereto, there is a cooling period of 4 hours. Thereafter, based on the amount and frequency of the transaction QnA or OTP is sent to the registered mobile number of the customer and the transaction is then authenticated by inserting the transaction password."

13. In the affidavit, the respondent no.4 has admitted that on 12/1/2020 and 13/1/2020, 7 (seven) beneficiaries were added to the petitioner's account using the credentials of the petitioner and the details of the beneficiaries are set out as below :-

Beneficiary Name	Beneficiary Bank	Tracker ID sent on
Sanjeev Das	HDFC Bank	12/01/2010 19:49
Chandan Balmiki	ICICI Bank	12/01/2020 19:42
Pooran Singh	YES Bank	13/01/2020 00:11
Pradeep Kumar	Oriental Bank of Commerce	13/01/2020 00:16
Rahul Ashok Pandey	Bank of Baroda	13/01/2020 19:35
Sahnaji Begam	Bank of Baroda	13/01/2020 23:58
Sajib Sardar	Bank of Baroda	13/01/2020 00:02

The affidavit further proceed to state that addition of the details of the beneficiaries, the tracker ID was sent on the registered mobile number of the Petitioner and a cooling period of four hours was observed before initiating the fund transfer. Thereafter, an OTP was also sent to the registered mobile number of the customer at the time of actual fund transfer and after inserting the transaction password, numerous transactions amounting to Rs.1.24 crores were made through petitioner's customer ID. The affidavit has set out the details of the transactions as below:-

Beneficiary Name	Beneficiary Bank	Date and time of transaction	Transaction amount
Sanjeev Das	HDFC BANK	13/01/2020 Time : 00:35:31.010 00:38:10.000 00:40:48.003 10:30:14.000 10:32:14.000 10:33:13.010	 9,00,000/- 9,00,000/- 7,00,000/- 10,00,000/- 9,00,000/- 2,00,000/-
Chandan Balmiki	ICICI Bank	12/01/2020 Time : 23:54:10.003	 9,50,000/-
Pooran Singh	YES Bank	13/01/2020 Time : 08:22:58.003	 10,00,000/-
Pradeep Kumar	Oriental Bank of Commerce	13/01/2020 Time : 08:26:07.003 08:34:12.003 09:09:43.010	 9,50,000/- 10,00,000/- 10,00,000/-
Rahul Ashok Pandey	Bank of Baroda	12/01/2020 Time : 23:42:58.010	 9,00,000/-
Sehnaj Begam	Bank of Baroda	13/01/2020 Time : 08:30:26.010	 10,00,000/-
Sajib Sardar	Bank of Baroda	13/01/2020 Time : 08:59:41.003	 10,00,000/-
		TOTAL	**1,24,00,000/-**

14. The affidavit filed on behalf of the Bank further state that out of 14 transactions, 11 transactions were carried out by using the petitioner's existing credentials and the transaction password of the petitioner was changed on 13/1/2020 at 9.12 a.m.

The affidavit further state that when the petitioner sought refund of the amount of Rs.1.24 crores, based on the Master Circular issued by Reserve Bank of India, on 6/7/2017, claiming that the petitioner has no liability since the unauthorised transaction has occurred without its negligence and the petitioner has intimated the Bank about the fraudulent transaction in three days, and since the service provider i.e. respondent no.5, without the consent of the petitioner, had issued a new SIM card, the Bank of Baroda vide its email dated 31/12/2021 forwarded its response. The Bank adopted a stand that the case is of 'suspected transaction' and such transactions are not possible without disclosure of confidential details.

It is the case of the Bank that it rendered all its cooperation to the police authorities, as it shared the details of the account beneficiary. It is a specific stand adopted by the Bank that it had ensured all necessary precautions by introducing multiple security layers for any successful online transaction to take place and not only this, it also assisted the customer in preventing further siphoning of the money.

In short, it is the case of Bank of Baroda that it is not responsible for making any payment, as the transaction is doubtful and the petitioner ought to have been vigilant.

15. The petition also received a response from respondent no.5 Service Provider, Vodafone Idea and its authorised representative has filed an affidavit on 3/2/2023, by asserting, at the outset, that no reliefs are sought against it and the

allegations levelled in the petition are unsubstantiated, when the petition suggest that the service provider did not verify the documentation and/or authorisation required for SIM exchange process.

The respondent no.5 admit that Mr. Ashok Jindal, CEO of the petitioner, subscribed to Mobile No. 9223391091 on 26/12/2019 and the affidavit is accompanied with the petitioner's postpaid customer application. It is also stated that since multiple numbers were subscribed to, for the purpose of use by the Company for its business, subscriptions were flagged as 'Company Owner Company Paid' (COCP).

A categorical statement is made in the affidavit that SIM exchange policy of the service provider differs in subscription flagged COCP vis-a-vis individual/personal subscriptions and COCP numbers have separate customer service agents handling their request along with a separate process that is to be followed, and this process is set out in the following words :

> "7.3 The COCP SIM Exchange Policy inter alia stipulates that when a customer service agent receives a call requesting a SIM exchange, an email is sent to the registered email ID requesting approval for such SIM exchange, the email also sets out the new SIM number as well as the mobile number for which such exchange is requested. The SIM exchange is processed only after receipt of approval. Moreover, the COCP SIM Exchange Policy stipulates that in the event the email ID is not registered on this respondent's systems, the SIM exchange request is to be rejected and the individual is to be directed to attend a store of this respondent along with requisite documents. This respondent craves leave to refer to and rely upon the COCP SIM Exchange Policy as and when produced."

16. As far as the procedure adopted in the present case is concerned, the affidavit state that, its Call Centre received a call

from number 9198293548 on 11/1/2020 at 6.26 p.m, requesting for SIM exchange of mobile no. 9223391091 and as per the COCP SIM exchange policy, the customer service agent requested the caller for verification of name and authorised email address associated with the number.

The caller presented himself as Mr.Ashok Jindal and provided the customer service agent with the authorised email address of the petitioner, i.e. hr@pnpind.com and since this information tallied with the information set out in the Consumer Authentication Form (CAF), the caller was informed that the SIM exchange would be made effective only upon receipt of the approval from the authorised email ID of the petitioner.

The affidavit is accompanied with the transcript of the call recording. It is therefore a categorical stand adopted by respondent no.5 that there is no negligence or malfeasance on its part and in fact it took all necessary steps, ensuring diligence in compliance with its COCP SIM Exchange policy.

The affidavit further state that on 16/1/2020, one Ms.Renuka Narkar, an employee of the petitioner company informed the respondent that the SIM number activated on mobile no. 9223391091 was not working and sought the reason for the same.

She was informed by the Customer Service Agent that a SIM exchange has taken place, owing to which SIM number 89910271001159369960 was no longer functional.

The customer agent then provided the details of the SIM exchange. Thereafter, Mr.Ashok Jindal addressed an email to Vodafone Idea, denying that he had ever made such request for SIM exchange and the response given by the customer service agent that the SIM exchange was not provided without his consent was being read in a completely different context. In para 7.14, Vodafone has adopted a specific stand as below:-

> "7.14 There is no question of any admission of liability on part of this respondent as evidently this respondent acted in terms of the COCP SIM Exchange Policy and the petitioner has not alleged any connivance on part of this respondent. That apart, the caller had evidently provided the requisite information in terms of the COCP SIM Exchange Policy and there was no cause for the customer service agent to seek further information given that the final approval for the SIM exchange was to come from the petitioner's authorized email ID as set out in the CAF."

17. Along with the affidavit, certain documents are annexed which include the application from Mr. Ashok Jindal for availing the postpaid services of the service provider for PNP Polytex Private Limited. The service provider has also annexed the purchase order for allotting mobile numbers to 42 user names in a plan under the designation 'Executive' and this include 9223391091 being allotted in favour of Renuka Sorap with SIM number 89910271001159369960 and this is the same number in respect of which Ms.Renuka Narkar made inquiries.

Further, the affidavit is also accompanied with an application for porting out certain numbers out of the corporate mobile number and this include mobile number 9223391091 which was sought to be ported out of the corporate mobile

number by request on 23/12/2019.

18. When the petitioner filed a complaint in Borivali police station, it was investigated and the statement of Dipak Sharma on behalf of the petitioner was recorded.

He referred to the two current accounts with the cash credit facility at Bank of Baroda, Jaya Talkies Branch, S.V. Road, Borivali, and stated that the accounts were registered with Vodafone Number 9223391091, which was registered in the company's name. He also sated that the Company does all transactions from the accounts by availing online facility.

According to the informant, on 13/1/2020, when he came to the Company and checked the bank account, he noticed that the login ID and password were blocked. He checked the bank account with another login ID and password, which is only for checking the bank account details and he found that between 12/1/2020 and 13/1/2020, various transfers had taken place and amount was diverted to some other account.

The investigation was conducted in the Cyber Crime complaint and upon completion of investigation, the charge-sheet is filed in the Competent Court by invoking Section 420, 465, 467, 468, 471, 120B r/w Section 34 of IPC against four accused persons i.e. Sanjeev Das, Jivanlal Singh, Ashok Gupta and Laxman Singh, and the charge-sheet also made a provision for further investigation in respect of other accused persons as the amount was transferred into various other accounts. The charge-sheet specifically allege that, the named accused persons

unauthorisedly transferred the amounts from the two bank accounts belonging to complainant to other accounts by manipulating the user name, password and transaction ID password. The charge-sheet also level the accusations that they have also changed the SIM card of the mobile number which was used by the Bank for the purposes of operating the bank accounts, so as to divert the amount from the said banks.

At the conclusion of the investigation, four persons are accused of colluding with each other in defrauding M/s.PNP Polytex Private Limited by swindling Rs.1.24 crores from its two Bank accounts with cash credit facility held by them in Bank of Baroda by changing the ID, transaction ID and password as well as changing the SIM number 9223391091 registered with the bank for these accounts. The charge-sheet also reveal that the Bank accounts where the money was transferred, was also opened by using fake documents.

19. The Reserve Bank of India has also filed an affidavit which has justified its communication addressed to the petitioner mentioning that there was no system lapse on part of the Bank and no deficiency in Banking service.

20. Responding to the affidavits filed by respondent nos.1, 4 and 5, the petitioner has filed counter affidavit, reiterating that the charge-sheet filed by Borivali police station on 11/4/2020 prima facie establish that online fraud was committed by third party breaches and the charge-sheet do not allege any connivance on part of the petitioner.

It is specifically stated that since the charge-sheet has specifically levelled an accusation that the fraudster had acquired duplicate SIM card belonging to the petitioner for using it to generate OTP which had given them unauthorised access to the petitioner's account, it is sufficient to establish that unauthorised transaction occurred due to third party breaches and therefore, Clause 9 of the Master Circular of RBI dated 6/9/2017 is attracted.

It is reiterated that the petitioner filed an FIR within one hour of the knowledge of the unauthorised transaction and even shared copy of the FIR with the Bank. It is also stated that pursuant to the filing of the FIR, four people involved in the fraudulent unauthorised transaction even got arrested by Mathura Police station and on culmination of the investigation, charge-sheet is filed, which contain material to establish that the account of the petitioner was manipulated and unauthorised transaction took place because of the connivance of all the accused persons.

21. We must mention that the whole object of the RBI issuing the circular/guidelines is to protect the customer, who has fallen prey to unauthorized transactions resulting in to debit of his account/card, when the transaction is effected through electronic banking. The Reserve Bank of India has issued directions to all scheduled commercial banks for strengthening their system and procedure, by introducing various

mechanisms, with an expectation that the system and procedure in the bank must be designed to make customers feel safe about carrying out electronic banking transactions and the RBI expected the Banks to adopt robust and dynamic fraud detection system.

One of the mode prescribed is the bank asking their customers to mandatorily register for SMS alerts and wherever available, register for e-mail alerts for electronic banking transactions. The RBI has made it mandatory that SMS alerts shall be sent to the customers, while e-mail alerts may be sent, wherever registered and simultaneously the customer must be advised to notify their Bank of any unauthorized electronic banking transaction at the earliest after the occurrence of such transaction, as longer time taken to notify the bank will pose high risk to the customer.

The Banks are directed to provide customers with 24 x 7 access through multiple channels for reporting unauthorized transactions that had taken place and/or loss or theft of payment instrument such as card, etc. and the bank shall also enable the customers to instantly respond to the SMS and e-mail alerts so that the customers are not required to search for a web page or an e-mail address to notify the objection. The swift action on part of the customers as well as the Bank is specifically underscored by RBI, since it is most important in determining the extent of the customer's liability.

Keeping this aspect in view, the Reserve Bank has fastened

zero liability on a customer, in case of third party breach when the deficiency lies neither with the bank nor with the customer, but lies elsewhere in the system and the customer notify the bank within three working days of receipt of communication from the bank regarding unauthorized transactions.

22. In our view, the circular of the RBI dated 06/07/2017 is independent of any criminal investigation to be conducted to establish any cyber crime, as the RBI intended to protect the customer who has suffered financial loss on account of fraudulent or unauthorized electronic banking transactions.

Without even a semblance of reference to any cyber investigation, the RBI deemed it appropriate to issue directions for limiting the liability of the customers in unauthorized electronic banking transactions and particularly, when the customer is not at fault. The burden to establish that the customer is at fault is on the bank and once a customer has notified the bank about the fraudulent transaction, from the date when he received communication from the bank, it is imperative for the bank to credit the amount involved in the unauthorized electronic banking transaction to the customer's account and if the reporting is within three days, then the liability of the customer is zero.

Since the burden of proving the customer's liability in respect of unauthorized electronic banking transaction is on the bank, we have to ascertain whether the HDFC Bank has discharged its burden.

23. Ms. Shilpi Jain, representing the petitioner had placed reliance upon the following decisions :-

(1) Pallabh Bhowmick Vs. The Ombudsman, Reserve Bank of India,[1]
(2) State Bank of India vs. Pallabh Bhowmick and ors,[2]
(3) Dadha Pharma LLP vs. Reserve Bank of India and ors,[3]
(4) Jaiprakash Kulkarni and ors Vs. The Banking Ombudsman and ors[4]
(5) Canara Bank Vs. Canara Sales Corporation and ors, AIR 1987 SC 1603.[5]
(6) Jindal Cocoa LLP and ors vs. Reserve Bank of India and ors,[6]

24. In **Jindal Cocoa** (supra), the Division Bench of this Court has emphasized upon the binding effect of the Master Circular issued by the Reserve Bank of India and applied the principle that the provisions therein must be purposively construed and a construction which erodes the very purpose of statutory instrument should always be avoided.

Keeping in mind the circular issued by RBI, which has emphasized on the Banks encouraging electronic banking and online transactions but at the same time, intending to have a mechanism in place to protect the customers against the risk arising out of unauthorised debits, the policy of the RBI covers the following :-

1 2022(5) GLT 292
2 2024 SCC Online GAU 1519
3 MANU/TN/2381/2025
4 2024 SCC Online Bom 1666
5 (1987) 2 SCC 666
6 2025 SCC Online Bom 21

> "Scope/Coverage : Electronic Banking Transactions generally covers transactions through following modes
> i) Remote/online Payment Transaction (e.g Mobile Banking Card not present Transactions, Internet Banking, Prepaid Payment Instruments etc)
> (ii) Face to face/Proximity Transaction (e.g ATM, POS, QR Code based transactions etc.)
> (iii) Any other transaction done by electronic mode and accepted by the Bank for debiting/crediting customer account."

25. The policy of the Reserve Bank of India, while construing the rights and obligations of a customer in case of unauthorised electronic banking transaction has clearly provided that where the customer is negligent and where he has shared the payment credentials, card number, expiry period, OTP, clicked on unknown links, 100% of the unauthorised electronic banking transaction will be the customer's liability and he shall have to bear the entire loss until he reports it to the Bank.

The policy also contemplated situations where the Bank is subjected to a regime and in some situations, it levied zero liability on the customer, who is entitled to get compensation from the Bank, which is limited upto the value date transaction amount of the unauthorised electronic banking transaction.

However, in case of third party breach – unauthorised electronic banking transaction, happened due to third party breach, the policy contemplate thus :-

> " 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."

26. In the circular of 6/7/2017, the Reserve Bank of India had cast zero liability on the customer in the following situation.

"6. A customer's entitlement to zero liability shall arise where the unauthorized transaction occurs in the following efents:
(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.

A customer is made liable for the loss by limiting the liability of the customer in the following scenario.

"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. Ar loss occurring after the reporting of the unauthorised transaction shall borne by the bank.
>
> (ii) In cases where the responsibility for the unauthorised electronic bank transaction lies neither with the bank nor with the customer, but 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."

27. In the present case, we have before us a full-fledged investigation carried out in the complaint filed by the Company and on completion of the investigation, the charge-sheet has been filed which has charged the accused persons of defrauding M/s.PNP Polytex Private Limited, by swindling Rs.1.24 crores from the two accounts i.e. (i) 03860500000078 and (ii) 03860500000106, with cash credit facility by changing the ID, transaction ID and password and even changing the SIM number and mobile number 9223391091 registered with the Bank for the two accounts.

Since now the investigating machinery has also come to a conclusion that it is the accused, who have defrauded the Bank, without attributing any negligence to the complainant company, according to us, nothing deserve to be proved more than this.

The lame excuse of the Bank of Baroda and the Reserve Bank to say that the mistake do not lie with the Bank, may be true as because of the SIM swapping, which is admittedly allowed by the respondent no.5, on the suspicion that the request was genuine, the messages sent by the Bank if any, were never received by the Petitioner. Merely stating that the

mobile phone was kept in a locker on the closing day and was seen by the authorised person of the company only on Monday, to find that the amount was swapped on 12/1/2020 and 13/1/2020 i.e. Saturday and Sunday and therefore, the Company is to be held liable, do not appeal to us at all.

28. The Vodafone Company has categorically admitted that there was request for change of the of the SIM on 11/1/2020 and the transcript annexed along with the affidavit of Vodafone would reveal that a person made a phone call from number 9198293548, representing that he was Ashok Jindal and he requested for SIM replacement. The Vodafone company without even putting a question as to why SIM replacement was sought for, obliged him by granting his request and this being allowed on 11/1/2020, the fraudulent transactions took place on 12/1/2020 and 13/1/2020.

When the SIM is replaced and made non-functional, obviously, no messages were received. In fact, Bank of Baroda ought to have been cautious in considering that the transactions were done on Sunday i.e. 12/1/2020 and in the early hours on 13/1/2020, when the Bank had not even opened, as from the details of transactions, as set out in the affidavit of the Bank itself, 12 transactions which took place on 13/1/2020 between 00:35:31.010 to 08:59:41.003.

The last transaction on 13/1/2020 was before the opening of the Bank. Rest of the transactions are done on

12/1/2020, which was Sunday.

29. It is not for the first time that the petitioner company was dealt with by the Bank and in fact, the Company had multiple accounts and on multiple occasions, huge amounts must have been withdrawn, transferred and definitely the transaction on Sunday and before the opening hours of the Bank i.e. 13/1/2020 itself made the transaction suspicious.

The 14 transactions were carried out by using the petitioner's existing credentials and according to Bank of Baroda itself, the transaction password of the petitioner was changed on 13/1/2020 at 9.12 am, after the amount was already dwindled off. It is also not the case of the Bank that the petitioner, the account holder insisted the amount to be permitted to be transferred with an hurry and between the closing hours on Saturday and the opening hours of the Bank on Monday.

Now, in the wake of the investigation report that the accused persons are responsible for the fraudulent transaction as they had hacked the system and by obtaining the details of the account, including the transaction ID, user name, password and they manipulated the whole transaction in a way that the messages are not received on the SIM card in possession of the petitioner company but are received by someone else, and therefore, the Bank as well as the petitioners were in dark when the transactions took place and the money was siphoned by the fraudsters.

30. Recently, we were confronted with a similar situation where the petitioner's account with HDFC Bank was debited by adopting a similar mechanism as the SIM Card of the petitioner was replaced on four occasions, without the approval of the petitioner, and though the Bank specifically adopted a stand that it had forwarded the SMS for every transaction, including addition of beneficiaries, increasing the transaction limit and ultimately the actual transfer into various accounts, no message was received by the petitioner. In the said case, there was no report of Cyber Crime, but the police machinery had concluded that it was a case of fraudulent transaction by swapping the SIM.

BSNL, the service provider had also filed the affidavit admitting that the SIM was changed on four occasions at different locations, though it adopted a stand that it was replaced following due verification procedure.

31. In the aforesaid background, we noted that it was a case of SIM swapping and in **Subodh Korde Vs. Union of India** and ors (WP No. 11990/2023), we have recorded thus:-

> "76. From the affidavit filed by BSNL, it is, therefore, clear that it is the case of SIM swapping. SIM swapping is a technique used by criminals to obtain a duplicate or clone of a SIM card linked with a phone number to impersonate identity of line holders and gain access to their bank account by sending an SMS (OTP Code) used as two factors authentication. BSNL has stated in its affidavit that since an application was made for SIM replacement on the count that the mobile phone was lost, a new SIM is provided with the same number and from the affidavit of BSNL, it is evident that the SIM was replaced on four occasions, right from 12/07/2021 to 15/07/2021.
>
> As far as the Petitioner is concerned, he admitted that there was some issue with his SIM card and he had approached the service

provider on 15th i.e. on one occasion.

The Indian Cyber Crime Coordination Centre (I4C), which is operated through Ministry of Home Affairs, has floated national cyber crime helpline 1930 (Call Immediately To Report
Fraud and Freeze Bank Accounts) and Sanchar Saathi Portal. The precautionary and safety tips and advisory from the Coordination Centre is, 'act on 'no signal'....if your phone suddenly loses signal unexpectedly, immediately contact your service provider'.

SIM swapping has received attention from the Ministry of Home Affairs as a sophisticated form of identity theft, where fraudsters take over a victim's phone number and this has been expressed to be a rising concern in India. The fraudsters collect personal details via phishing social media or previous data licks and they adopt procedure of impersonation. The fraudsters tricks the mobile operator claiming the SIM is lost/damaged and request for a new one and in such a scenario, the victim's actual SIM loses connectivity (no network). The fraudsters then receive OTPs and banking alerts on the new SIM enabling them to drain bank accounts, often by bypassing two fold authentication. The net-banking frauds involve access to the bank account basic details and the mobile number and then approaching the service provider, impersonating the owner of the number with fake papers and a request to swap the SIM. After verification, the service provider deactivate the old SIM and the fraudsters get access to the new active mobile SIM, when the original one fails to operate as a result all financial SMS, OTP alerts as regards the transactions are arrived on new active card, which is in the hands of the fraudster.

This is precisely the methodology, which has been adopted here and this is evidently clear to us from the affidavit of BSNL, as the Petitioner has pleaded that he faced trouble in connectivity and even approached to his service provider and his SIM was replaced. That is the specific reason why the Petitioner did not receive any OTP on 14th or 15th when the beneficiaries were added or the financial limit of transaction was increased and the actual transaction took place on 15/07/2021 and it is obvious that the message must have been received on a cloned/duplicate SIM and the Petitioner did not receive any message/OTP.

In no case, we find that the Petitioner was careless or that he had shared the password with anyone and ultimately the burden is upon the bank to establish that he was careless or negligent, which the bank in our view, has failed to establish.

77. In consonance of the circular dated 06/07/2017, since the Petitioner has not contributed to the fraud nor he was negligent and he immediately reported about his accounts being debited, or he receiving only one message and that too, after a lapse of time and with the specific stand of the BSNL, reflecting that there was swapping of his SIM card, according to us, the Petitioner is a victim of cyber fraud. The transactions from his account, including addition of beneficiaries, increase of TPT limit and the debit of the amount from his two accounts through eight transactions were all unauthorized. Surprisingly, the Bank, despite the alert created, has not taken any

> serious steps and has adopted a stand simplicitor that it had discharged its obligations, once it sent OTPs. The Petitioner never received the OTPs nor did he receive any e-mail communication in respect of the unauthorized transactions.
>
> The reason now is very clear, being that his SIM card was cloned/swapped and, therefore, somebody else other than him, has received the OTP and probably, shared the OTP so as to authenticate the transaction. The Petitioner, however, acted promptly, once he realised that some amount is debited to his account and he reported the matter to the higher officer and did whatever was possible to him to do. The Petitioner is, therefore, entitled for the benefit of 'zero liability', as we do not conclusively say that the Bank was deficient, but it appears that the Bank was casual in stating that it had sent the OTP and put the blame on the Petitioner, of being negligent in sharing the password, which the Petitioner never did."

32. While pronouncing the aforesaid decision, we have also made reference to the decision cited before us from Guwahati High Court in case of **Pallabh Bhowmick** (supra) where the benefit of RBI Circular dated 6/7/2017 was claimed by the petitioner, a practising Advocate, holding a saving bank account in SBI, Guwahati Branch and who was duped by Rs.94,204/- by three separate online transactions.

The facts reveal that petitioner had made online purchase of some garment from 'Louis Philippe' store which he wanted to return and get the money back. When he received a call from fraudster to identify himself as Customer Care Manager of Louis Phillipe and asked the petitioner to download on mobile app for refund of the amount in lieu of the return of garment and when the petitioner did so, the amount of Rs.94,204/- was debited to his account.

The petitioner immediately informed the Customer Care Centre of SBI, with a request to cancel the three transactions and the debit card of the petitioner was blocked. An FIR was

also registered which invoked Section 417 and 420 of IPC and he also made a complaint to the SBI about the fraudulent transaction and lodged complaint with Cyber Crime Cell, Criminal Investigation Department, Assam.

The Bank denied its liability which constrained the petitioner to approach the Court and the learned Single Judge held thus :-

> **"21.** As per clause 9, which deals with reversal timeline of zero liability/limited liability of customers in case of unauthorized electronic banking transaction, it would be the discretion of the bank to waive off any customer liability even in case of negligence of the customer. From a conjoint reading of the aforementioned clauses of the circular, it can be inferred that in case of un-authorized electronic transactions the Bank would have a duty to reverse the payment and credit the amount involved in the un-authorized transaction within a time frame, provided the fraudulent transaction is reported by the Customer within the time frame provided in the Circular. In an appropriate case, even the negligence, if any, on the part of the customer, can be waived by the Bank.
>
> **22.** From the pleadings available on record it is evident that the three online transactions from the petitioners account took place on 18.10.2021 when he had downloaded the 'mobile app' on being prompted by the fraudster. The petitioner had done so in order to get refund of his money from "Louis Philippe". The aforesaid three transactions were evidently unauthorized as the petitioner never intended to transfer any amount to the respondent No. 4 by downloading the mobile app. The respondent No. 2 has also not denied that the transaction was unauthorized. Therefore, merely because the petitioner had downloaded the mobile app, that cannot by itself lead to the presumption of negligence on the part of the petitioner in assisting the unauthorized transaction. Had the Bank installed effective cyber security system and online fraud control measures then in that event, even if a mobile app is downloaded by a customer, money could not have been transferred from the bank account without proper authorization. Regardless of whether it was a UPI or PG transaction, it is not believable that the petitioner would deliberately share his OTP, password and MPIN so as to allow his hard earned money to be siphoned off from the bank account by a fraudster, that too, on three consecutive occasions, in quick successions. Rather, the incident appears to be pure and simple case of cyber crime whereby, the fraudster had hacked the database of respondent No. 3 and thereafter, got access to sensitive information pertaining to various customers of "Louis Philippe" including the petitioner which information was used for completing the fraudulent transactions. The participation on the part of the petitioner appears to be only to the extent of downloading the mobile app. Although the respondent No. 2 has contended that the petitioner had shared OTP, password and MPIN with the fraudster, yet, the said claim could not be

substantiated by the Bank. Nothing has been stated in the counteraffidavit filed by the respondent No. 2 to indicate as to when, how and in what manner the OTP, MPIN and password was shared by the petitioner with the fraudster. No material particulars of the complicity on the part of the petitioner have been furnished in the affidavit. Therefore, this court is of the view that the respondent No. 2 Bank has completely failed to establish any negligence on the part of the writ petitioner."

33. The Division Bench of the Guwahati High Court upheld the said decision by recording that the incident appeared to be pure and simple case of cyber crime, whereby the fraudster has hacked the database of respondent No.3 and got access to the sensitive information pertaining to the customers of the bank, which was used for completing the fraudulent transaction. Recording that the participation of the petitioner appears to be only to the extent of downloading the 'mobile app', it was held that the bank had failed to establish any negligence on part of the petitioner. The observation of the Division Bench reads thus:-

"40. ...The Banks cannot absolve themselves of the liability towards losses suffered by the customers on account of unauthorized electronic transactions based on perceived negligence of the customers. In the present case, having considered the facts and circumstances of case and the materials available on record, we concur with the view of the learned Single Judge, that the appellant has failed to establish negligence on the part of the respondent no.1/petitioner leading to the fraudulent transactions. Thus, the learned Single Judge has rightly directed the appellant to deposit an amount of Rs.94,204.80/- (Rupees Ninety-four thousand two hundred four and Eighty Paisa) only, in the bank account of the respondent no.1/petitioner."

Worth it to note that the Hon'ble Apex Court while dismissing the Appeal made very pertinent observations and we deem it appropriate to reproduce the same.

"2. We are in complete agreement with the observations as contained in

Para 42 of the impugned judgment referred to above.

3. All that the High Court has said is that the original petitioner who suffered the loss was not negligent in any manner. All transactions relating to the account of the respondent No.1 -herein maintained with the petitioner - Bank were found to be unauthorized and fraudulent. It is the responsibility of the bank so far as such unauthorized and fraudulent transactions are concerned. The Bank should remain vigilant. The Bank has the best of the technology available today to detect and prevent such unauthorized and fraudulent transaction. Further, clauses 8 and 9 respectively of the RBI's Circular dated 6-7-2017 make the position further clear.

4. We also take notice of the fact that within 24 hours of the fraudulent transaction, the customer, i.e., the respondent No.1 - herein brought it to the notice of the Bank.

5. We expect the customers, i.e., the account holders also to remain extremely vigilant and see to it that the O.T.P.s generated are not shared with any third party. In a given situation and in the facts and circumstances of some case, it is the customer also who could be held responsible for being negligent in some way or the other."

34. One more decision of this Court cited before us is in case of **Jai Prakash Kulkarni**, (supra) where in the backdrop of the Circular of the Reserve Bank of India, the lost amount was directed to be deposited in the petitioner's account.

35. It is in the wake of the aforesaid legal situation and the factual scenario emerging before us, we are of the opinion that the petitioner in this case, cannot be blamed at all, as from the report of the investigation, it is evident that the petitioner Company was defrauded by the fraudsters by swapping the Sim and Vodafone Company has admitted that it permitted the SIM to be replaced and therefore, obviously no message was received by the petitioner on the registered mobile number and it is clear from the investigation report that the message was shared on another SIM, which was duplicate/cloned and

obviously the OTP which was sent was shared by the fraudster and the transactions were permitted. No fault lies with the petitioner company and it promptly reported about the transaction to Bank of Baroda, Reserve Bank of India as well as the concerned police station which carried out an investigation and even filed the charge-sheet.

In our view, this is a fit case where the petitioner is entitled for the benefit of fastening of zero liability as per the Circular of RBI dated 6/7/2017, as the unauthorised transaction has taken place, without any contributory fault/ negligence/deficiency on part of the Bank or the customer i.e. the petitioner, but it is a case of third party breach, where on the basis of a duplicate SIM being issued to the fraudsters, the OTPs were secured and the Bank being unaware that the OTPs are shared not with the petitioner company, but with some third party stranger, beneficiaries were allowed to be added and the two accounts of the petitioner company were debited in the sum of Rs.1.24 crores.

Out of the said amount, an amount of Rs.47,81,750/- has been prevented from being disbursed in favour of the fraudsters. Since the petitioner as a customer, is entitled to the benefit of the circular of Reserve Bank of India, casting zero liability, but the Bank of Baroda as well as the Reserve Bank has failed to remit the amount to the petitioner's account, we deem it appropriate to direct the Bank of Baroda to credit the accounts of the petitioner with the amount which has been

debited on 12/1/2020 and 13/1/2020, and if some amount is still lying in the Bank which has not been disbursed and informed to be frozen i.e. a sum of Rs. 47,81,750/- the Bank is directed to appropriate that amount, as the petitioner Company is entitled for only the sum of which its two accounts are debited. Since the petitioner has been deprived of the said amount without any fault of its, we direct the amount to be credited with an interest @ 6% from the date when the petitioner made a complaint to the Bank.

36. The amount shall be credited into the accounts of the petitioner Company within a period of eight weeks from today.

Petition is made absolute in the aforesaid terms.

(MANJUSHA DESHPANDE, J) **(BHARATI DANGRE, J.)**