2019 PLRonline 3401

Kerala High Court

HIGH COURT OF KERALA AT ERNAKULAM

JUSTICE A.MUHAMED MUSTAQUE

TONY ENTERPRISES V. RESERVE BANK OF INDIA

WP(C).No.28823 OF 2017(C)

11.10.2019

Cyber fraud – SIM Swap Fraud – Is a fraud using a duplicate SIM card issued by the mobile service provider against the registered mobile number – Using the duplicate SIM card provided by the mobile service provider, one time passwords generated through the banking system are obtained by fraudsters to operate another person's bank account – Fraudsters also commit fraud on mobile service providers by providing fake identity cards to obtain duplicate SIM cards.[Para 9]

Cyber fraud – Identity theft – SIM Swap Fraud – SIM Swap Fraud 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 – Under Section 66 of Information Technology Act, identity theft is a penal offence – It states that whoever fraudulently or dishonestly uses an electronic signature, password or any other unique identification of any other person is liable to be punished with imprisonment- Information Technology Act, Section 66. [Para 9]

SARFAESI Act – Fraud – In cases that contain allegations of fraud, the matter goes out of bounds of the SARFAESI Act – Bank, then, is liable to prove its claim against the persons who have committed fraud – The Bank in such cases cannot adjudicate their claim and decide against the borrower. [Para 11]

Cyber fraud – It is for the bank to secure the safety of online banking transactions – Banking transaction is both contractual and fiduciary – The bank owes a duty to the customer. Both have a mutual obligation to one and another – The bank, therefore, is bound to protect the interest of the customer in all circumstances. [Para 13]

Reserve Bank of India – Master circular dated 6.7.2017 – 'disputed transaction' – Protecting customers in unauthorised electronic banking transactions – A 'disputed transaction' has to be understood as a transaction prima facie tainted by fraud – Classifying transaction as such would depend upon the nature of allegations and investigation carried out in this regard – Classification of such transaction must be with reference to the events identified by the RBI – That means the very validity of the transaction is at stake – A mere challenge made by the customer would not be sufficient – If such a challenge is supported by the report of an independent investigation pursued by the Police or other such agencies, that would prima facie establish that it is a 'disputed transaction' – If the report indicates that the online transaction was carried out by some other person other than the customer or on his behalf, that has to be treated as a 'disputed transaction'. [Para 14]

Reserve Bank of India – Master circular dated 6.7.2017 – 'disputed transaction' – 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.[Para 20]

Reserve Bank of India – Circular dated 4.1.2019 – RBI/2018-19/101 – Rights of the parties – Limits the liability of the customer – The circular does not foreclose the remedy of the bank to proceed against the fraudsters and also against customers or any other persons or entity involved – It also does not prevent a customer from proceeding against the bank through a civil suit if he was unable to lodge complaint within the time as provided in the circular – Civil rights of the parties if otherwise available are not lost based on the circular, though the circular has statutory backing – The circular only indicates the nature of the action to be taken by the bank when there are complaints relating to an unauthorised payment transaction. [Para 15]

Reserve Bank of India – Circular dated 4.1.2019 – RBI/2018-19/101 – Cyber fraud – The bank cannot recover the amount from the customer stating that the customer was negligent in protecting his personal details – If such personal details were exposed due to the laches on account of the action on the part of the customer, it can at the best be treated as negligence. To what extent the customer can be made responsible for such negligence is a matter of probe and adjudication through a civil suit. [Para 15]

Reserve Bank of India – Circular dated 4.1.2019 – RBI/2018-19/101 – Cyber fraud – Zero liability – Sim Swapping – Police investigation prima facie established that fraud has been committed – The beneficiaries hail from West Bengal – There is nothing on record to establish any connivance on the part of the petitioners – The police investigation also would reveal that the accused obtained duplicate SIM cards by using fake identity cards – It was also brought out that the beneficiaries immediately withdrew the money from their bank accounts at West Bengal – In such circumstances, the transactions can be treated as 'disputed transactions' – These transactions would fall within the sweep of zero liability as referred to in RBI Circular – The remedy of the bank in such circumstances is to approach the civil court and recover the amount from the persons who were responsible for such transactions – Money taken out from accounts of the customers ordered to be restored. [Para 21]

JUDGMENT

The banking sector has adopted technology for the efficiency of the banking business and also for faster and hassle-free customer service. Technology enables the service provider to offer customers and clients a plethora of benefits that allow them to dispense with their physical presence for banking transactions. The growth of the banking sector by use of technology has also given rise to a new form of fraud using counter technologies against the bank. Technology provides services without boundaries. Geographical location is no longer a constraint due to the onset of the use of technology. The convenience of service without boundaries and access to service from anywhere is the aim of any business. Criminals and fraudsters also have grown at the same pace as that of the growth of technology. Criminals are also now able to disguise their location and operate from anywhere in the world. The use of technology has resulted in the dissemination of personal data. Data can no longer be stored as done in a brick and mortar system. Data is bound to be exposed in different forms depending upon the nature of the service provided. Technology has its own set of advantages and pitfalls. Data theft in Cyber Law means stealing another person's confidential or personal information without his consent or authority. The online banking service of a customer is linked with his email and mobile number. This is essentially used to authenticate banking transactions of the customers. Fraudsters having knowledge about this authentication method, have devised fraud using SIM cards and email. These two cases before me depict a case of SIM swapping fraud to gain access to bank accounts of the petitioners and to withdraw money from their bank accounts. The petitioners allege fraudulent transactions by the third parties to withdraw money from their accounts online. Since the point of law involved in both these writ petitions is one and the same, it is appropriate to dispose of both these writ petitions by

way of common judgment.

2. W.P.(C).No.28823/2017 has been filed by Tony Enterprises and Tony Lites, a proprietary firm and a partnership firm respectively, both of which have a cash credit account at Chittoor Road branch of Oriental Bank of Commerce. The petitioners had also availed the online banking facility of the Bank, the alerts in respect of which would be sent and were linked to the mobile number of one Mr.Tony Davies, the sole proprietor of the first petitioner and the Manager of the second petitioner. On 8th June, 2017, Mr.Tony Davies came to realize that a total amount of Rs.16,25,000/- had been unauthorizedly transferred from the accounts of the petitioners by way of online transactions effected through the online banking app of the Bank. The registered mobile number of Mr.Tony Davies had become dysfunctional on 6 th June 2017 and he had approached the service provider, M/s. Idea Cellular on 7th June 2017 to enquire regarding the same. He was told by the representative of M/s.Idea Cellular that his number had become dysfunctional as a duplicate SIM card had been issued in respect of the number on 6th June 2017 upon the request of a person who had fraudulently represented himself as Mr.Tony Davies. Upon subsequent restoration of network services after re-issuance of a duplicate SIM, he reaslised that such amounts had been unduly transferred to several accounts from the bank accounts of the petitioners.

3. W.P.(C).No.28824/2017 has been filed by one Mr.Cherian C.Kariparambil and a partnership firm called MINDSTRONG HR Solutions. The first petitioner has overdraft facility account with South Indian Bank and the second petitioner has a current account with HDFC Bank. The petitioners had also availed the online banking facility of the Bank, the alerts in respect of which would be sent and were linked to the mobile number of the first petitioner who is also the Managing Partner of the second petitioner-firm. On 28 th April 2017, Mr.Cherian came to realize that a total amount of Rs. 23,00,000/- had been unauthorizedly transferred from the accounts of the petitioners by way of online transactions effected through the respective online banking apps of the Bank. Mr.Cherian’s registered mobile number had become dysfunctional on 25th April 2017 and he had approached the service provider, M/s BSNL Telecom on 27th April 2017 to enquire regarding the same. He was told by the representative of M/s BSNL Telecom that his number had become dysfunctional as a duplicate SIM card had been issued in respect of the number on 25th June 2017 upon the request of a person who had fraudulently represented himself as Mr.Cherian by furnishing ID proofs belonging to him. Upon subsequent restoration of network services after re-issuance of a duplicate SIM, he realized that such amounts had been unduly transferred to several accounts from the bank accounts of the petitioners.

4. The petitioners in both these writ petitions approached this Court with similar prayers. They seek a declaration to the effect that they have zero liability in the light of the Circular issued by the Reserve Bank of India. The petitioners also sought a direction to the bank to make good the loss suffered by them.

5. The Bank entered appearance and filed a counter affidavit. They have taken the stand that the login ID, password and telecom number are only known to the petitioners and that without laches on their part, others cannot operate their account. The Bank further states that all the transactions were initiated and completed upon proper validation of customer credentials. It is their case that a one time password was generated through the mobile number linked with the account and that the transaction was validated upon furnishing the one- time password (OTP) so generated through the system. It is also stated that all fund transfers were authenticated through the OTP which was also sent to the email addresses of the petitioners as well.

6. These writ petitions were originally filed without impleading the Mobile Service Provider. Their role is crucial in understanding the modus operandi of the transfers so effected. This Court, therefore, directed the petitioners to implead the service providers. In W.P.(C).No.28824/2017, the Bharat Sanchar Nigam Limited (BSNL) was impleaded as an additional respondent and, in W.P.(C).No.28823/2017, M/s.Vodafone Idea Ltd was also impleaded as an additional respondent.

7. In the counter affidavit filed by BSNL, it is stated that an individual claiming to be Cherian C.Karippaparampil the writ petitioner in W.P.(C).No.28824/2017 approached the office of BSNL on 27.4.2017 for replacement of SIM. The individual concerned apparently

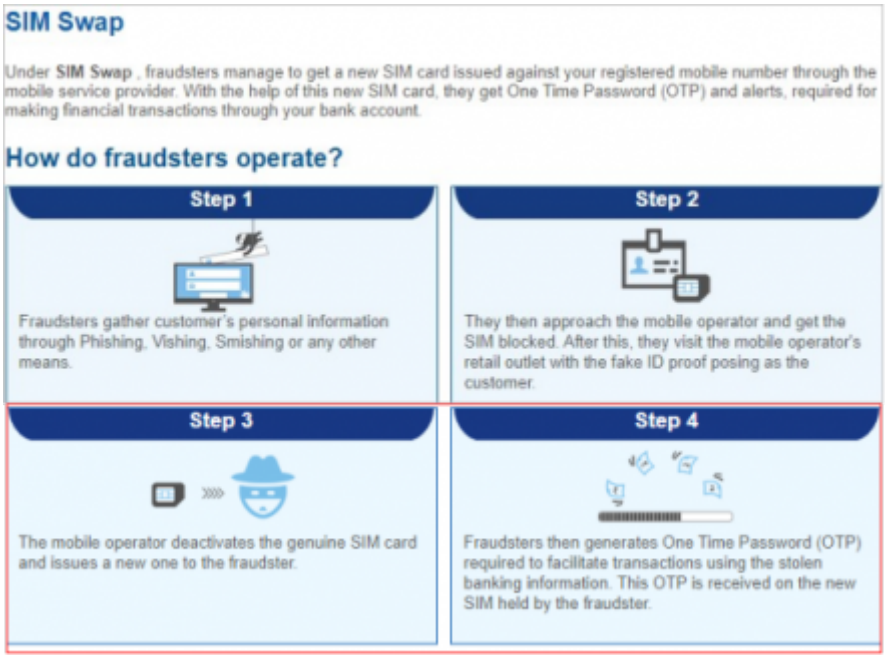
also produced his original driving licence and handed over the Xerox copy of the driving licence to obtain the duplicate SIM card.

8. Tony Davies, the first petitioner in W.P.(C).No.28823/2017 and Cherian C.Karippaparampil, the writ petitioner in W.P. (C).No.28824/2017 have registered complaints with the local police who registered FIR under Sections 406 and 420 of the Indian Penal Code. The investigation was later transferred to the Crime Branch Crime Investigation Department's Organized Crime Wing (CBCID OCW) at Ernakulam. A Detective Inspector of the CBCID OCW-II pursued the investigation thereon and after examination of several witnesses and obtaining statements from them, came to the conclusion that the amounts had been transferred to several bank accounts in West Bengal and Maharashtra by fraudsters based in West Bengal. The reports of the investigating officer were made available before this Court. It is stated therein that the investigating officer registered a crime against persons hailing from West Bengal. He has also stated in his reports that the fraudsters followed the same modus operandi in the case of accounts of both the petitioners to transfer the amounts by acquiring duplicate SIM cards belonging to Mr.Tony Davies and Mr.Cherian by means of fraudulent misrepresentation and using it to generate OTPs which would give them unauthorized access into the petitioners' online banking facilities. By verifying the IP address of the accused, the Detective Officer came to the conclusion that the accused illegally logged into the bank account of the complainants and transferred the amount from the complainants' accounts. It is also stated that the transferred amounts were immediately withdrawn from the beneficiary accounts at West Bengal and Maharashtra. The investigation reveals a case of SIM swapping and identity theft.

9. For deciding the issue in hand, this Court has to go through SIM swap fraud in banking transactions:

i. SIM Swap Fraud: SIM swap fraud is a fraud using a duplicate SIM card issued by the mobile service provider against the registered mobile number. Using the duplicate SIM card provided by the mobile service provider, one time passwords generated through the banking system are obtained by fraudsters to operate another person's bank account. Fraudsters also commit fraud on mobile service providers by providing fake identity cards to obtain duplicate SIM cards.

ii. In the website of HDFC Bank, SIM swap is narrated as follows:



iii. SIM Swap Fraud 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. Under

Section 66 of Information Technology Act, identity theft is a penal offence. It states that whoever fraudulently or dishonestly uses an electronic signature, password or any other unique identification of any other person is liable to be punished with imprisonment.

10. This Court, while considering the matter under public law remedy must confine its inquiry to the action of the Bank on the basis of public law parameters. This Court cannot adjudicate the dispute in like manner as done in civil adjudication. The Court has to tread a cautious path while considering a matter under Article 226 of the Constitution. If any attempt is made to find out the liability based on the available records placed before this Court, it would amount to acting beyond the power under Article 226 of the Constitution. The question, therefore, that arises is in what manner public law remedy could be invoked to deal with the matter invoking allegations of fraudulent banking transaction. This assumes so much importance in the wake of the securitisation enactment which gives the Bank a power to determine and decide the liability in the case of banking transactions. The SARFAESI Act confers power/right on the Bank to enforce any security interest created in their favour without the intervention of the Court or the Tribunal, in accordance with the provisions of Section 3 of the SARFAESI Act. As per the provisions of the SARFAESI Act, the onus of discrediting the claim of the Bank lies on the customer who can do so by filing an appeal against the action taken by the Bank. Before the enactment of the securitisation act, the Bank would assert claims only through the adjudication process of the civil court. The civil court can very well address all issues including the fraudulent transactions or unauthorised transactions.

11. Enforcement of security interest as referable under the SARFAESI Act would arise only when a borrower is under the liability to a secured creditor under a security agreement and when he makes default in repayment of any such secured debt (See Section 13.2 of the SARFAESI Act). This liability clearly refers to liability under a contract. It is based on such contractual obligation that a borrower is deemed to be proceeded against when a default is committed in repaying the loan amount. In a matter covered under the contractual obligation, the onus to disprove the liability under the SARFAESI Act as adverted above is on the borrower by means of challenging the action under Section 17 of the SARFAESI Act. However, in cases that contain allegations of fraud, the matter goes out of bounds of the SARFAESI Act. The Bank, therefore, is liable to prove its claim against the persons who have committed fraud. The Bank in such cases cannot adjudicate their claim and decide against the borrower. The question, therefore, that arises is whether the Bank can proceed against the borrower based on an assumed liability or not when there is a serious challenge to a banking transaction on the ground of fraud. This is a delicate question. The Court has to weigh the interest of the bank as well as that of the borrower while deciding the issue. In every transaction, if it is alleged that there was a fraud, the bank would be denuded of its power to invoke statutory provisions under the SARFAESI Act. Therefore, the Court has to consider in what circumstances, a transaction can be termed as a 'disputed transaction' that requires independent adjudication.

12. The Reserve Bank of India issued a master circular dated 6.7.2017 protecting customers in unauthorised electronic banking transactions. The circular states that a customer has zero liability in the following events:

"(i) Contributory fraud/negligence/deficiency on the part of the bank (irrespective of whether or not the transaction is reported by the customer)

(ii) Third party breach whether deficiency lies neither with the bank nor with the customer but lies elsewhere in the system and the customer notifies the bank within three working days of receiving the communication from the bank regarding the unauthorised transaction".

The events referred therein are only illustration. It cannot be said the list as above is exhaustive. The circular proceeds based on assumed facts and circumstances. It refers to contributory fraud, negligence deficiency etc. It does not indicate about liability when there is a dispute to the events as above. In that background, the question also arises as to the remedy of the bank to recover the amount under the 'disputed transaction'.

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 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(Encryption: the process of converting information or data into a code, especially to prevent unauthorized access), this security encryption can be hacked using different methods. The welknown 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 (Wifi Snooping: stealing data from unsecured WiFi network. Convert (information or data) into a code, especially to prevent unauthorized access.) 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.

14. Defining a 'disputed transaction':

A 'disputed transaction' in this context has to be understood as a transaction prima facie tainted by fraud. Classifying transaction as such would depend upon the nature of allegations and investigation carried out in this regard. "No man is bound by a bargain into which he has been induced by fraud to enter, because assent is necessary to a valid contract." (See KERR On the Law of Fraud and Mistake 7 th Edition). The author further states that the transaction so induced is not void but only voidable at the election of the party defrauded. Classification of such transaction must be with reference to the events identified by the RBI. That means the very validity of the transaction is at stake. A mere challenge made by the customer would not be sufficient. If such a challenge is supported by the report of an independent investigation pursued by the Police or other such agencies, that would prima facie establish that it is a 'disputed transaction'. If the report indicates that the online transaction was carried out by some other person other than the customer or on his behalf, that has to be treated as a 'disputed transaction'.

15. Remedy of the Bank:

The bank has a remedy by way of filing a civil suit for claiming the loss suffered in the transaction and to recover it from the person responsible. In common law jurisdiction fraud is a tort and considered as a civil wrong. It is also a penal offence under the relevant statutory provisions. The circular of the RBI presumes in such circumstances, 'zero liability' to the customer. A recent circular issued by the RBI, RBI/2018-19/101, dated 4.1.2019, limits the liability of the customer. It reads thus:

"Limited liability of a customer:

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.

The above shall be clearly communicated to all PPI holders."

The circular as above does not foreclose the remedy of the bank to proceed against the fraudsters and also against customers or any other persons or entity involved. It also does not prevent a customer from proceeding against the bank through a civil suit if he was unable to lodge complaint within the time as provided in the circular. Civil rights of the parties if otherwise available are not lost based on the circular, though the circular has statutory backing. The circular only indicates the nature of the action to be taken by the bank when there are complaints relating to an unauthorised payment transaction. The bank also cannot recover the amount from the customer stating that the customer was negligent in protecting his personal details. If such personal details were exposed due to the laches on account of the action on the part of the customer, it can at the best be treated as negligence. To what extent the customer can be made responsible for such negligence is a matter of probe and adjudication through a civil suit.

16. It is profitable to refer to the observations of the House of Lords *in London Joint Stock Bank, Limited v. Macmillan and Arthur* [1918 AC 777] which is as follows:

"As the customer and the banker are under a contractual relation in this matter, it appears obvious that in drawing a cheque the customer is bound to take usual and

reasonable precautions to prevent forgery. Crime, is indeed, a very serious matter, but everyone knows that crime is not uncommon. If the cheque is drawn in such a way as to facilitate or almost to invite an increase in the amount by forgery if the cheque should get into the hands of a dishonest person, forgery is not a remote but a very natural consequence of negligence of this description."

The learned Lord Chancellor observed further at page 795 as follows:

"Of course the negligence must be in the transaction itself, that is, in the manner in which the cheque is drawn. It would be no defence to the banker, if the forgery had been that of a clerk of a customer, that the latter had taken the clerk into his service without sufficient inquiry as to his character. Attempts have often been made to extend the principle of Young V. Grote (1827) 4 Bing. 253, beyond the case of negligence in the immediate transaction, but they have always failed."

17. Placing reliance on *Macmillan's case* (supra), the Apex Court in *Bihta Co-operative Development and Cane Marketing Union Ltd. v. Bank of Bihar* [AIR 1967 SC 389] held as follows:

"11. "The principle of this case cannot help the respondent before us. If the signatures on the cheque had been genuine so that there was a mandate by the customer to the banker but the cheque was somehow got hold of by an unauthorised person and encashed by him, the bank might have had a good defence. If the signatures on the cheque or at least that of one of the joint signatories to the cheque are not or is not genuine, there is no mandate on the bank to pay and the question of any negligence on the part of the customer, such as, leaving the cheque book carelessly so that a third party could easily get hold of it would afford no defence to the bank..."

18. The Apex Court in *Canara Bank v. Canara Sales Corporation & Ors* [AIR 1987 SC 1603], after referring to the judgments in *Macmillan's case* (supra) as well the judgment of the Apex Court in *Bank of Bihar* [AIR 1967 SC 389] at para 42 held as follows:

42. We adopt the reasoning indicated above with great respect. Unless the bank is able to satisfy the Court of either an express condition in the contract with its customer or an unequivocal ratification it will not be possible to save the bank from its liability. The banks do business for their benefit. Customers also get some benefit. If banks are to insist upon extreme care by the customers in minutely looking into the pass book and the statements sent by them, no bank perhaps can do profitable business. It is common knowledge that the entries in the pass books and the statements of account sent by the bank are either not readable, decipherable or legible. There is always an element of trust between the bank and its customer. The bank's business depends upon this trust."

19. A learned Single Judge of this Court in similar circumstances had held in R.S.A.No.1087/2018 as follows:

"...In short, there is also no difficulty in holding that if a customer suffers loss in connection with the transactions made without his junction by 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, and the banks are, therefore, liable for the loss caused to their customers..."

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.

21. In the present case, the police investigation prima facie established that fraud has been committed. The beneficiaries hail from West Bengal. There is nothing on record to establish any connivance on the part of the petitioners. The police investigation also would reveal that the accused obtained duplicate SIM cards by using fake identity cards. It was also brought out that the beneficiaries immediately withdrew the money from their bank accounts at West Bengal. In such circumstances, the transactions can be treated as

‘disputed transactions’. These transactions would fall within the sweep of zero liability as referred to in RBI Circular. The remedy of the bank in such circumstances is to approach the civil court and recover the amount from the persons who were responsible for such transactions.

22. As have come out of the pleadings, amounts have been debited from the loan account of the petitioners. The petitioners cannot be held responsible for such debit without establishing through the civil court that they are responsible for such withdrawal from the loan account. If any amount deposited by the petitioners also have been transferred, in the same manner, that shall be restored to the petitioners without any delay at any rate within two weeks from the date of receipt of a copy of this judgment. These directions are issued without prejudice to the bank to proceed against the persons who are responsible for these transactions through civil court. These writ petitions are disposed of accordingly. No costs.