IN THE HIGH COURT OF JUDICATURE AT MADRAS

Reserved on	27.02.2023
Pronounced on	28.04.2023

CORAM

THE HON'BLE Ms. JUSTICE R.N.MANJULA

WP.No.6789 of 2021
and
WMP.Nos.7343 & 7345 of 2021

Dr.R.Pavithra .... Petitioner

Vs.

1.The Commissioner of Police,
Office of the Commissioner of Police,
Vepery,
Chennai-600 007.

2.The Additional Director General of Police,
CB-CID,
CID Headquarters,
24, Pantheon Road,
Egmore,
Chennai-600 008.

3. The Deputy Superintendent of Police,
CB-CID Cyber Crime Branch,
CID Headquarters,
24, Pantheon Road,
Egmore, Chennai-600 008.
[R2 and R3 deleted vide order dated 17.03.2021]

4.The Deputy Commissioner,
K-4 Anna Nagar Police Station,
Anna Nagar,
Chennai.

5. The Inspector of Police,
K-8 Police Station,
Arumbakkam,
Chennai.

6.The Reserve Bank of India,
16, Rajaji Salai,
Fort Glacis,
Chennai.

7.The City Union Bank,
Vigilance Department,
703, Anna Salai,
Chennai.

8. The Assistant General Manager,
City Union Bank,
Vigilance Department,
24-B, Gandhi Nagar,
Kumbakonam 612 001.

9.The Manager,
City Union Bank,
Irungalur Branch,
Opposite SRM Campus,
Irungalur, Trichy.

10. PayTM Mobil Solutions Private Limited,
B-121, Sector 5,
Noida-201301, India.

11.State Bank of India,
Rajaji Road,
Mannadi, Chennai Port Trust,
Chennai 600 001.

12.Fincare Small Finance Bank,
292, New No.116, Z Block II Avenue,
Beside Tower Metro Station,
Anna Nagar,
Chennai 600 040.
[R11 and R12 suo motu
impleaded vide order dated 02.11.2022] .... Respondents

Prayer :- This Writ Petition is filed under Article 226 of the Constitution of India for issuance of Writ of Certiorari Mandamus, praying to call for the records of the proceedings in CO/VIG/1365/2020-21 dated 01.03.2021 on the file of the 7th respondent, and to quash the same as illegal and without jurisdiction, and consequently to direct the 3rd and 4th respondents to conduct a free and fair investigation into the cyber crime complaint given by the petitioner dated 15.02.2021.

Prayer in WMP.No.7343 of 2021: This Writ Miscellaneous Petition is filed under Article 226 of the Constitution of India, praying to issue an Advocate-Interim Direction directing the respondents 7-9 to immediately credit a sum of Rs.3 lakhs, being the sum unlawfully and authorizedly siphoned off from the account of the petitioner in accordance with the circular of the 6th respondent dated 06.07.2017 and bearing No.RBI/2017-18/15, pending disposal of this Writ petition.

Prayer in WMP.No.7345 of 2021: This Writ Miscellaneous Petition is filed under Article 226 of the Constitution of India, praying to issue an Advocate-Interim Direction directing the respondents 4 & 5 to file a status report on the status of the investigation conducted by them in connection with the complaint of the petitioner dated 15.02.2021.

For Petitioner : Mr. Sharath Chandran

For Respondents : Mr.A.Gopinath,
Government Advocate (crl.side) for RR1,4 & 5
: RR2 & 3 deleted vide order dated 17.03.2021
: Mr.V.S.Rishwanth for Mr.T.Poornam for R6 CRBI
: Mr.S.R.Sundar for RR7 to 9
: Mr.Shivakumar and Suresh for R10
: Mr.B.Sivakollapan for R11
: Mr.D.Sathiyaraj for R12

ORDER

This Writ Petition has been filed to issue a Writ of Certiorari Mandamus to call for the records of the proceedings in CO/VIG/1365/2020-21 dated 01.03.2021 on the file of the 7th respondent, and to quash the same as illegal and without jurisdiction and consequently to direct the 3rd and 4th respondents to conduct a free and fair investigation into the cyber crime complaint given by the petitioner dated 15.02.2021.

2.The brief facts of the case is as under:

The petitioner was a post graduate at the SRM Medical College at Trichy. During her post-graduation, the petitioner was serving as a resident doctor to attend the patients affected with COVID-19. She was being paid with a stipend of Rs.25,000/- per month by SRM Medical College, Trichy and the amount would be credited to her bank account with the 8th respondent. Out of the said earnings, she had saved a sum of Rs. 3,20,000/- and was planning to utilise the same to meet her final year fees during April-2021. On 10.02.2021 the petitioner returned to Chennai as she was not well. On 09.02.2021 an attempt was made by some miscreant to hack into her savings account, bearing No.500101011835967 with the 7th respondent bank.

2.1.The said fact was known to her through an alert SMS. She noticed the said message only on 11.02.2021, on which date she received another SMS alert at 14:15 hrs and 22:15 hrs**.** She immediately sent a message at 22.59 hours to the Bank asking them to block the account. She was under the impression that the account had been blocked pursuant to her request.

Once again, on 13.02.2021, she received another SMS informing her that there had been an attempt to break into her savings account. The petitioner sent another message to the bank along with her registered mobile number, requesting the bank to block her account.

2.2. In fact, she had issued messages to block her account only as she had been instructed through the alert messages. Again, on 15.02.2021 at 12.33 p.m., she received an SMS informing her that someone had hacked her account. Within a few minutes, there was an unauthorised debit from her account for a sum of Rs.50,000/- followed by another sum of Rs.1,00,000/- at 12.43 pm and yet another sum of Rs.50,000/- at 12.44 pm and one more Rs.1,00,000/- at 12.45 pm. The miscreants had hacked her account and stolen her money. The petitioner called the 7th respondent bank at 12.43 pm itself and asked them to block her account. However, her money had been illegally siphoned off; no OTP for withdrawal has been received on her mobile phone and she has not shared her bank details or personal details with anyone. Thereafter, she rushed to the City Union Bank at Aminjikarai branch and lodged a written complaint. This was

acknowledged by the bank at 2 p.m. on the very same day, and she had also given a police complaint to the 4th respondent at 3 p.m. on the same day. She received the information from the City Union Bank at Aminjikarai branch that her money had been transferred fraudulently to the PayTM account. Immediately, she called PayTM and registered a complaint. The money was taken away from her account and transferred to the accounts of some unknown accused. PayTM had shared the customer ID, bank account details, etc. of the accused through P2P wallet transfers. The money appeared to have been illegally transferred from her account to six accounts in the State Bank of India and Fincare Small Finance Bank, Bangalore and the accounts are said to be belonging to one Uthham Kumar and one Balram Kumar of Mathiya Pradesh and Uttar Pradesh, respectively. On 15.02.2021 the accused person attempted once again to hack the account and an SMS alert was received by her at 18.30 hours. Immediately, she had called the City Union Bank at the Aminjikarai branch and they advised her to reset her mobile PIN and to enable BIOMETRIC authorization. She received another SMS message at 21.26 hours that the reset was successful. However, on 16.02.2021 the accused once again illegally logged onto the petitioner's

account; since the transfer of funds had been blocked, he was not able to transfer the funds. So it traces a suspicion about the security system of the 7th respondent bank, and there is also a possibility that any insider of the banker also has got a connivance.

2.3. On 16.02.2021, at about 15.10 pm, she received a message stating that the accused had once again logged onto her account. So the petitioner called the bank and informed them, and thereafter her account was completely blocked. The City Union Bank at Aminjikarai branch has been utterly careless during the entire process. However, the 7th respondent has sent a letter dated 01.03.2021 denying its liability to refund the loss sustained by the petitioner. The bank was fully aware of the request made by the petitioner to block her account on 11.02.2021 itself, and now they are shifting the blame upon the petitioner. The petitioner has enclosed the messages she has received. The City Union Bank at Aminjikarai branch now seeks to fulfill its responsibility under the RBI's circular dated 06.07.2017. If the complaint is given within 3 days, there is zero liability on the part of the customer. Hence, the petitioner is entitled to get the reversal

of Rs.3,00,000/- loss suffered due to the fraud committed on her account. Instead of honouring the application, the City Union Bank at Aminjikarai branch has attempted to shift the blame on the petitioner, and this raises a suspicion whether the branch officials themselves have any complicity in the mischief. In view of the stress and shock suffered due to the above incident, the petitioner suffered a miscarriage on 22.02.2021. The petitioner has filed this petition seeking a Writ of Certiorarified Mandamus to quash the impugned proceedings of the 7th respondent and further directions.

3. The 6th respondent is the Reserve Bank of India (hereinafter referred to as the RBI), the 7th respondent is the City Union Bank and the 10th respondent is PayTM. Even though the petition was filed only against the 10th respondent, the State Bank of India and Fincare Small Finance Bank have also been *suo moto* impleaded as parties to the proceedings by virtue of the orders of this Court dated 02.11.2022. However, the existing respondents 2 and 3, who are the Additional Director General of Police, CBCID, and the Deputy Superintendent of Police, CBCID, have been deleted by order dated 17.03.2021.

4. The RBI has filed the counter by stating that the responsibility of the RBI is to regulate and supervise the banking sector to the benefit of the economy in the country under the provisions of the Banking Regulation Act 1949. Various directions and guidelines have been issued by the Reserve Bank of India to regulate the functions of banking entities. In the matter of transactions between the regulated entities and their customers, the RBI does not interfere. Only in the event that the regulated entity violates or contravenes the directions issued by the RBI, the latter would take cognizance of the matter. However, if the customer approaches the RBI Ombudsman under the Ombudsman Scheme, the same will be examined within the ambit of the scheme and appropriate redressal will be given within the scheme.

4.1. The petitioner had filed a complaint before the RBI Ombudsman in Chennai under the Banking Ombudsman Scheme -2006 [herein after referred as the BOS-2006], inter alia, alleging that the money in her savings bank account, maintained by the 7th respondent, was siphoned off through multiple unauthorised debits on February 15, 2021. After perusing the

documents and comments from the bank, i.e., City Union Bank, the Ombudsman closed the complaint under clause 13(a) of the BOS-2006 by observing that there is no deficiency observed against the bank on the services as mentioned in clause 8 of the Ombudsman Scheme. Clause 8 of the Ombudsman Scheme enumerates various grounds in which a person can file a complaint against the bank. The RBI has issued directions and guidelines to both Prepaid Payment Providers and banks for customer protection and has defined the extent of the liability of the customers and the relevant regulated entity. The RBI had issued a circular dated 04.01.2019 vide No. DPSS.CO.PD.No.1417/02.14.006/2018-19 and it is applicable to all Authorized Non Bank Prepaid Payments Instrument Issuers for Customer Protection/limiting the liability of customers in unauthorised Electronic Payment Transactions through Prepaid Payment Instruments (PPIs) issued by Authorized Non-banks.

4.2. Paragraph 6(b) of the below mentioned circular, states about the customer's liability in cases where the deficiency lies neither with the PPI issuer nor with the customer but elsewhere in the system and the customer

notifies the PPI issuer or the customer regarding the unauthorised payment transaction. For the sake of argument, the said paragraph is extracted as follows:

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

Customer Liability in case of Unauthorized Electronic Payment Transactions through Paypointz Wallet		
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 unauthorized 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 unauthorized transaction by the customer to the PPI issuer -	
	i. Within three days#	Zero
	ii. Within four to seven days#	Transaction value or Rs.10,000/- per transaction, whichever is lower
	iii. Beyond seven days#	Full liability of the customer
(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 unauthorized transaction to the PPI issuer. Any loss occurring after the reporting of the unauthorized 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 unauthorized 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"

4.3. In the same circular, it is stated that the burden of proving customer liability in cases of unauthorised electronic payment transactions

shall lie on the PPI issuer.

4.4. The 6th respondent, RBI, had also issued a circular dated 06.07.2017 bearing circular number DBR.No.Leg.BC.78/09.07.005/2017-18 applicable to All Scheduled Commercial Banks (including RPBs), All Small Finance Banks and Payments for Customer Protection/ Limiting Liability of Customers in unauthorised Electronic Banking Transactions. Under paragraphs Nos. 6 and 7 of the above circular dated July 6, 2017, the bank is liable in cases where the responsibility for the unauthorised electronic banking transactions lies neither with the bank nor with the customer but elsewhere in the system. The relevant portion of the circular is also extracted hereunder:

> "**Limited Liability of a Customer**
>
> **(a) Zero Liability of a Customer**
> 6. A customer's entitlement to zero liability shall arise where the unauthorised transaction occurs in the following events:
> (i) Contributory fraud/ negligence/ deficiency on the part of the bank (irrespective of whether or not the transaction is reported by the customer).
> (ii) Third party breach where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, and the customer notifies the bank within three working days of receiving the communication from the bank regarding the unauthorized transaction.
>
> **(b) Limited Liability of a Customer**
>
> 7. A customer shall be liable for the loss occurring due to unauthorized 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 unauthorized transaction to the bank. Any loss occurring after the

reporting of the unauthorized transaction shall be borne by the bank.

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

Table 1

Maximum Liability of a Customer under paragraph 7 (ii)	
Type of Account	**Maximum liability (Rs.)**
• BSBD Accounts	5,000
• All other SB accounts • Pre-paid Payment Instruments and Gift Cards • Current/ Cash Credit/ Overdraft Accounts of MSMEs • Current Accounts/ Cash Credit/ Overdraft Accounts of Individuals with annual average balance (during 365 days preceding the incidence of fraud)/ limit up to Rs.25 lakh • Credit cards with limit up to Rs.5 lakh	10,000
• All other Current/ Cash Credit/ Overdraft Accounts • Credit cards with limit above Rs.5 lakh	25,000

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

8. Overall liability of the customer in third party breaches, as detailed in paragraph 6 (ii) and paragraph 7 (ii) above, where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, is summarized in the Table 2:

Table 2

Summary of Customer's Liability

Time taken to report the fraudulent transaction from the date of receiving the communication	**Customer's liability (Rs.)**
Within 3 working days	Zero liability
Within 4 to 7 working days	The transaction value or the amount mentioned in Table 1, whichever is lower
Beyond 7 working days	As per bank's Board approved policy

The number of working days mentioned in Table 2 shall be counted as per the working schedule of the home branch of the customer excluding the date of receiving the communication "

4.5. Paragraph No.12 of the circular dated 06.07.2013 is similar to that of paragraph No.10 of the circular dated 04.01.2019 issued to all authorized non bank, Pre Paid payment issuers. According to Paragraph No.12 of the circular dated 06.07.2017 also the burden of proving the customer's liability in case of unauthorized electronic banking transactions shall lie on the bank.

5. **The main contesting respondents are 6th and 10th respondents and the counter of the 7th respondent is in brief:**

The 7th respondent /the City Union Bank submitted that the petitioner has suppressed and misinterpreted several material facts. The present cash

transactions have taken place by using the mobile payment application through a Unified Payment Interface (UPI). The petitioner has been using one such UPI ie. Pay TM app, who is impleaded as 10th respondent in this case. As per the guidelines laid down by the RBI vide master directions dated 18.02.2021, the use of the mobile application is fortified by multilayer protection. Any user using the UPI through its applications, such as Google Pay, Amazon Pay, PayTM etc., has to first complete the KYC [Know Your Customer] formality and only then he is allowed to use the UPI. The UPI is registered with the mobile number. The UPI can be used only if the user is using the same mobile number that has been registered in the bank with which he accedes his bank account. After registering the UPI with the mobile numbers only, the user can use the mobile applications for transferring money, making payments, or doing any kind of shopping, both physically and on-line.

5.1.The payments are secured by " Two Factor Authentication" [2FA] or Dual Factor Authentication. It is a security process in which users are provided with two different authentication factors to verify themselves. The

UPI typically has a 4 to 6 digit numeric pin (MPIN). In some cases, it is also a fingerprint, followed by an One Time Password (OTP). It is sent directly to the registered mobile number of the user. The MPIN, ATM PIN are set by the user and known only to the user, and the OTP is accessed only through the registered mobile number. The authentication process is only under the control of the user and no one else, unless it has been accessed by an unauthorised third party. All these processes are totally automated, and there is no human intervention at any level. The only way that could be compromised is if the details in the UPI are accessed by a third party by way of hacking.

5.2. In the case in hand, the petitioner had lost her money through PayTM i.e. 10th respondent herein, and not from the seventh respondent's system. The perpetrators had gained access to the petitioner's bank account through PayTM and not through the 7th respondent's bank system. The petitioner's bank statement would show that the petitioner has been regularly using PayTM for on-line shopping as well. On 09.02.2021 there was a login from an unauthorized third party. Immediately an SMS was sent at15:17:19

hours to the petitioners registered mobile number. The Message is as under:

> **" You have logged into your CUB Mobile Banking on 09.02.2021 15:17:19 IST. If not, send SMS as : BLOCK XXXX to 9281056789 from your regd mobile to block Mobile Banking.-CUB"**

5.3. The multiple Short Messaging Service (SMS) messages were sent every time there was an attempt to log into the petitioner's account. The generation and communication of the SMS are automated by the systems in real time, with no human intervention. The SMS Log report would show that multiple attempts have been made since 09.02.2021 and every time an attempt has been made, a message has been sent to the petitioner's registered mobile number. The number of SMS sent from the bank with dates is tabulated under:

Sl#	Date	No of SMS
1	09.02.2021	5
2	10.02.2021	1
3	11.02.2021	3
4	13.02.2021	4
5	14.02.2021	1
6	15.02.2021	20 (for every action)

5.4. The petitioner never took cognizance of the SMS that was sent on 09.02.2021. However, she saw these messages only on 11.02.2021. When

repeated messages are sent on February 11th, 13th, 14th, and 15th, 2021, the petitioner ought to have called the bank's customer care number and escalated the issue immediately by blocking her account. But the same was not done by her. The RBI's circular dated 06.07.2021 referred to by the petitioner will not be applicable to the present case because the entire issue is with the UPI service provider, i.e., PayTM, the 10th respondent herein. Moreover, it has to be ascertained if the petitioner's phone has been hacked. Without asserting these facts, the 7th respondent cannot be held liable.

5.5. It is seen from the reports that the petitioner's phone has been hacked by some third party. Every time the petitioner tried to change the MPIN, the hackers managed to access her account. If the phone is hacked, it is beyond the control of the bank to protect the account. The perpetrators had gained access to the petitioner's account through the 10th respondent and not this respondent's banking system on both occasions, i.e., 09.02.2021 and 11.02.2021. With regard to the mobile banking block request sent by the petitioner on 11.02.2021, nothing could be done. Since SMS request sent by the petitioner was in an incorrect format it was rejected. In fact the

petitioner was alerted immediately by the system by sending SMS to use correct format as under:

11-02-2021 22:29:21:923	Send block request with your netbanking user id
11-02-2021 22:29:21:945	Send block request with your netbanking user id

5.6. The SMS alert sent by the petitioner was not received by the bankers system since it was not correct. The following four unauthorized transactions had happened on 15.02.2021:

Amount	Time	Biller reference number	Journal Number	PG	Application
50000	15-02-2021,12:39:50	20210215145660900000	202357804	Paytm	MB
100000	15-02-2021,12:42:56	20210215146219000000	202365270	Paytm	MB
50000	15-02-2021, 12:44:20	20210215146232600000	202328578	Paytm	MB
100000	15-02-2021,12:50:43	20210215145580800000	202425495	Paytm	MB

5.7 All these transactions were done through a third-party app (PayTM) by using mobile banking login and second factor authentication as Card & PIN. The reported fraudulent transactions are PayTM transactions done using Mobile Banking (MB) ID and authorised with MB PIN for login, and Card PIN was used for second factor authentication for the transaction. The process for executing transactions in a third-party application is as

below:

a) Login to the third-party application

b) Choose the product like load wallet / recharge / purchase goods & services

c) Payment option would be displayed like Third party Wallet account (if money already loaded / Debit Card / Credit Card / BHIM UPI / Netbanking

5.8. Despite the efforts of the bank to secure the account of the petitioner by helping her to change the MPIN number, the perpetrators managed to get access. Even after the MPIN was changed by the petitioner, the hackers still managed to gain access to her account. On 15.02.2021 the hackers again attempted to access the petitioner's account; the petitioner ought to have sent her mobile for forensic examination. The petitioner could have immediately called the customer care number to block her account by reporting the unauthorised transactions. The petitioner has not reported the matter to PayTM, which is the main gateway from where the unauthorised transactions had taken place. There is no lapse on the part of the 7th respondent. The petitioner had also raised a complaint with the Banking Ombudsman. The hacking has actually taken place on 16.02.2021 and not

on 16.03.2021. The 6th respondent had issued a press release dated 11.03.2022 debarring the 10th respondent from adding any further customers until RBI completes its IT audit of the 10th respondent. There are issues with the 10th respondent, i.e., PayTM's mobile application, that could have led to this incident. The petitioner ought to have given a complaint to the 10th respondent, PayTM.

6. **<u>The 10th respondent PayTM has filed his counter and the 10th respondent's counter in brief is as under</u>**:

PayTM Payments Bank Limited, a company incorporated under the provisions of the Companies Act, 2013. It is a payment bank and is part of the new set of differentiated banks introduced by the Reserve Bank of India with the aim of extending deposit and payment services to millions of unbanked and under banked Indians. It has been granted with a licence by the Reserve Bank of India to carry on payment bank business under the Banking Regulation Act, 1949. This is also in line with the government of India in digitalizing payments and facilitating banking operations. So far as the PayTM payment bank is concerned, the petitioner has been impleaded

only as a proforma party and no specific allegations or grounds have been raised by the petitioner against the PayTM payment bank.

6.1. The 10th respondent is not a bank or other authority under Article 12 and hence it is not amenable to any writ jurisdiction. There is no privity of contract between the respondent No.10 PayTM payments bank. The 10th respondent is a mere facilitator and an on-line conduit provider for payments, having no technical or otherwise controlling control over the secured transactions. The transactions through on respondent No.10 is on a web based platform and mobile application have been verified by the CVV and the One-Time Password (OTP) of the credit and debit cards of the holders. The OTP has been delivered to the mobile number registered with such credit and debit card service providers and once the same is verified by the issuing bank and subsequent to the receipt of information from such a bank regarding the validity of the mode of payment, the technical server of respondent No. 10 automatically allows the order / transaction to be done. It is within the purview of respondent No. 10 to monitor or control any authorization or non-authorization of the on-line payments, which happen

through the server automatically.

6.2. All transactions carried out on the PayTM Platform are secured and require authentication of the OTP / PIN, before initiation, which is generated by the respective card /Bank service provider and known only to the individual customer / card holder / petitioner. If there had been any discrepancy in the execution of said transaction, such as a wrong card number / Account No., OTP/UPI PIN etc, the said transaction could never have been successful and the amount in question in said transaction could have never been transferred to any account. PayTM bank is a conduit service provider, and hence, in case any customer is willing to perform any transaction through the PayTM platform, he has to select the mode of payment, i.e., Debit/Credit card, net banking, UPI and upon entering correct and genuine banking credentials along with OTP / PIN etc., the said transaction takes place automatically without any manual intervention.

6.3. The RBI in its directions dated 06.07.2017(RBI/2017-18/15) on Customer Protection/Limiting Liability of Customers in Unauthorised

Electronic Banking Transaction has clearly specified that the customer shall be liable for the loss occurred due to unauthorised transactions if the loss was due to the negligence of the customer by sharing the payment credentials, etc., Neither in the petition nor in the legal notice, no grievance has been made against the respondent No.10 and hence the 10th respondent is not a necessary or proper party to these proceedings. The petitioner has an alternate efficacious remedy by approaching the adjudicatory authority under the Information Technology Act and the writ petition is barred in view of the alternate remedy. The 10th respondent has already provided the necessary information sought from him.

6.4. As per the ratio laid down by the Hon'ble Supreme Court in **State of Rajasthan V. Bhawani Singh & Ors, AIR 1992 SC 1018,** if there are disputed and mixed questions of fact that cannot be adjudicated in writ proceedings; the petitioner ought to approach the Information Technology, Adjudicatory Authority which is a designated authority for such on-line frauds.

7. Mr.Sarath Chandran, learned senior counsel for the petitioner submitted that there are materials to show that the impugned transactions were fraudulent and it was not done by the petitioner; even though the RBI guidelines have made it clear that if a complaint about fraudulent transactions is done within three days, the customer does not have any liability and it is the liability of the bank or Prepaid Payment Instructions (PPI) to make good the loss suffered by the customers; the unfortunate petitioner who held her account with the 7th respondent, City Union Bank, was defrauded by some fraudsters to withdraw money from her account by using PayTM applications.

8. Mr.S.R.Sundar, learned counsel for the respondents 7 to 9, denied their liability by stating that there was no deficiency of service on the part of the 7th respondent bank and hence the 7th respondent is not liable to compensate the loss suffered by the petitioner due to the fraudulent transactions. Apart from the branches of the banks through which a customer normally operates money transactions, now-a-days many payment banks have been introduced by the RBI. The aim of such a promotion of

payment banks is to extend deposit and payment services to unbanked and under banked Indians.

9. The above submissions adduced by the learned counsels of either side heard and the materials perused.

10. Even though the public is encouraged to use payment banks such as PayTM, Google Pay, Amazan Pay, etc., the customer is made to run from pillar to post, in case he is affected due to any 3rd party violations or fraudulent intervention. What is surprising is that even when the RBI has issued detailed master directions for both banks and Prepaid Payment Instruments [PPI], every institution shifts the blame upon the other and no one has come up with a concrete idea as to who has to bear the loss suffered by the petitioner, for none of her mistakes.

11. There were certain attempts made by some miscreants to access the petitioner's account with the City Union Bank through the PayTM app from 09.02.2021. The City Union Bank had alerted her by sending an SMS

that her account was accessed by someone. The petitioner happened to notice the message on 11.02.2021 and she had sent an SMS to block her account. But it was unsuccessful. The fraudulent attempts were continuing, and things went beyond the control of the petitioners and the bankers.

12. On 15.02.2021 the fraudsters had siphoned off nearly Rs.3,00,000/- from her account by making successive transactions using the PayTM application. It is the contention of the 7th respondent that their liability ends with alerting the customer and they were not able to block her account because the SMS was not sent in a proper manner. The petitioner omitted to call the branch directly to see that her account is blocked. After the advent of on-line transactions, the life style of the individuals has changed to a greater extent. The practice of establishing physical meetings with the branch has become obsolete. In view of the various online mechanisms provided by the banks for almost all banking services, no one goes to the branch physically in order to make any complaint. So it is not a surprise that the petitioner did not make any direct contact with the bank and that she followed scrupulously how she was instructed in the alert SMS.

13. A police complaint was given by the petitioner and it was registered with much difficulty. As per the status report submitted by the 4th respondent, the fraudsters were identified by their names and they have accounts with SBI. The fraudsters had acted smartly by transferring the amounts to the various accounts after doing the fraudulent transaction in order to prevent the reversal. After the complaint was made to the 7th respondent, he contacted the 10th respondent, PayTM, by stating that the fraudsters had used the PayTM mobile app and managed to access the PayTM account of the petitioner from some other mobiles.

14. In order to register as a PayTM user, one has to have a bank account and mobile number. After installing the PPI applications, the customer has to link his registered mobile number with his bank account and the application. By opening the app, either by using a biometric method or a PIN number, the app will be accessed and transactions will be done by typing the PPI-PIN numbers and the money can be transferred within moments. No doubt such applications are time saving and convenient, but

the user does not know how to address his grievance if anyone tampers with the accounts by fraudulent means and siphons off the money lying in his account.

15. The fradulent transactions were not done by the petitioner. It is neither the case of the 7th respondent bank nor the 10th respondent PayTM that the transactions were done by the petitioner herself, and she is making fraudulent claims. In fact, the investigation has revealed information about the persons involved and in the status report it is stated that the fraudsters have managed to access the app by being in some other states, like Bihar. Whatever might be the modus operandi adopted by the fraudsters, the fact remains that it was not the petitioner who had revealed the details of her PIN Number or other details to the fraudsters either knowingly or unknowingly. The fraudsters had used PayTM application and not the net banking/mobile banking of the 7th respondent bank to swindle money from the petitioner's account. So it is claimed by the 7th respondent that there is no security compromise at their end, and hence, the banker is not liable to compensate the petitioner.

16. The records would make it clear that the access was done through a payment bank named PayTM. In fact, with the details furnished by the 7th respondent and the 10th respondent as to the transactions, the investigation officer could know the persons who transacted and who made the fraudulent transactions and to whose accounts the money was so transacted and transferred. Fortunately, a sum of Rs.70,000/- was withheld by Fincare India, and after a series of court orders, Fincare India was obliged to reverse the said sum to the petitioner's account. Since the City Union Bank and PayTM shifted the blame upon each other and did not come forward to take up the responsibility of compensating the petitioner, the 6th respondent, RBI, has been asked to come out with their stand and to clarify who is liable to compensate the petitioner, as per their guidelines.

17. The 6th respondent, RBI, has filed his counter affidavit and stated about the various guidelines issued by the Reserve Bank of India in the interest of customer protection. The counter affidavit of the RBI was also diplomatic to the extent that the RBI did not pinpoint either the 7th respondent or the 10th respondent as a person who is liable to compensate

the petitioner. The above exercise of fixing the liability was left to the court in light of the guidelines of the RBI, which the 6th respondent reiterated in his counter. In fact, the RBI guidelines are customer-friendly, and if the customer happens to report about the fraudulent transactions within three days of the occurrence, as per the guidelines, there is 'ZERO LIABILITY' fixed on the customer. The above position is similar for both banks and Prepaid Payment Instruments, except for the fact that they were through different circulars. Since the transaction was not done through any `Net Banking sites but through a payment bank application by name ' PayTM', it has to be seen whether the banker or the payment banker is liable.

18. The case in hand does fall within the clause (b) of the following portion of the circular dated 04.01.2019 vide No. DPSS.CO.PD.No.1417/02.14.006/2018-19, which is applicable to all authorised non-bank Prepaid Payment Instrument issuers for customer protection/limiting the liability of customers in unauthorised electronic payment transactions in prepaid payment instruments (PPIs) issued by authorised non-banks. For the sake of clarity, paragraph No. 6 of the

circular reads as follows:

Customer Liability in case of Unauthorized Electronic Payment Transactions through Paypointz Wallet		
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 unauthorized 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 unauthorized transaction by the customer to the PPI issuer -	
	i. Within three days#	Zero
	ii. Within four to seven days#	Transaction value or Rs.10,000/- per transaction, whichever is lower
	iii. Beyond seven days#	Full liability of the customer
(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 unauthorized transaction to the PPI issuer. Any loss occurring after the reporting of the unauthorized 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 unauthorized 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"

19. The liability of the customer is fixed at Rs.10,000/- per transaction if the complaint has been made within 4 to 7 days and if beyond 7 days, it is as per the policy of the prepaid payment instrument issuer. In the case in hand, the petitioner had given her complaint to her banker immediately after the transaction. It cannot be claimed by the 10th respondent, PayTM, that

the petitioner ought to have given her complaint to the 10th respondent instead of the 7th respondent. Because even the petitioner was not able to know how the fraud was committed. The matter came to light after the initiative taken by the 7th respondent bank. In fact, the 7th respondent bank has been communicating with PayTM about the fraudsters' activity. So it cannot be said that the 10th respondent is not aware of the fraud just because the customer gave her complaint to her bank directly.

20. Another convenient submission made by the 10th respondent is that the 10th respondent payment bank is a private corporation and not a government institution, and hence, it cannot be subjected to the jurisdiction of this Court. The 6th respondent RBI, has stated that the primary function of the RBI is to regulate and supervise the banking sector for the benefit of this country's economy under the provisions of the Banking Regulation Act 1949. It is further submitted that the RBI would not normally interfere with the transactions between the regulated entities and their customers. But that this would not preclude the RBI from taking cognizance of the matter when the regulated entity violates or contravenes the RBI guidelines.

21. It is further submitted that the customer could approach the RBI Ombudsman under the Ombudsman Scheme and the same will be examined and appropriate actions would be taken for redressal of such grievances even if they fall within the ambit of the Scheme. Since a customer's savings habits or mode of money transactions could have an impact on the country's economy, it cannot be said that the customer's interest is alien to the interest of the economy of the country. If all the customers switch over to physical mode of money transactions and abstain from doing transactions through the banking sector, that would grossly affect the economy of the country and hence, the customer's interest is also paramount. So, the RBI has an obligation to safeguard the customer's interest as well. This is especially true when it comes to the knowledge of the RBI that a payment bank like PayTM evades to comply RBI guidelines and shrieks away its liability to compensate the petitioner in tune with the guidelines of RBI.

22. Even though the petitioner has sought compensation from the 7th respondent banker, the facts and materials available on record as discussed

above would only fix the liability on the payment bank [the 10th respondent] and not upon the 7th respondent bank. Though a straight away directions can not be given against the 10th respondent, since it is a private body, this Court can mould the relief in such a way that directions should be given to the 6th respondent, RBI, to take action against the 10th respondent for violating its own guidelines. The RBI guidelines are issued not as a formality, but the entities subjected to the RBI regulations should comply with the conditions of the master circular in its true letter and spirit.

23. In fact, as per the guidelines No. 16.4.8, the non bank Prepaid Payment Instrument issuers shall ensure that a complaint is resolved and the liability of the customer is established within the said time not exceeding 90 days. But the 10th respondent has not come forward to take cognizance of the grievances suffered by the petitioner, who was the user of the PayTM banking services. It is further stated in the above guidelines that if the PPI issuer is unable to resolve the complaint and determine the customer's liability within 90 days, the amount as prescribed under guideline No. 16.4.8 shall be paid to the customer irrespective of whether the negligence is on the

part of the customer or otherwise.

24. In the case in hand the 10th respondent had failed to resolve the dispute within 90 days and he has not come out with any concrete structure as to how the loss suffered by the petitioner is going to be compensated. Within 90 days from the date of the complaint i.e. from 16.02.202,1 the 10th respondent did not prove how the customer is liable. In fact with the informations furnished by the 7th respondent and the 10th respondent itself, it is made clear that there is no fraudulent actions on the part of the petitioner but the violations were done by the 3rd parties.

25. In fact, Mr.Sarath Chandran, learned counsel for the petitioner, has brought to the attention of this Court that it is at the discretion of the payment banks to waive the customers liability, if any, even if the customer had filed a complaint at a belated stage. It is further submitted that a Corporate Company by name One 97, which owns the consumer brand PayTM, along with PayTM Payments Bank Ltd have filed a writ petition before the Delhi High Court for seeking directions against the department of

telecommunications and the Telecoms Regulatory Authority of India to ensure complete and strict implementation of the provisions of telecom Commercial Communications Customers Preferences/Regulations 2018 and any other regulations issued from time to time to curb fraudulent unsolicited commercial communications sent over the respective their networks in order to prevent the customers of PayTM from suffering loss on account of fraudulent calls and messages containing either a link or phone number. Such frauds are committed thorough spying activities done by using the telecommunication services such as SMS and calls. It is conceded by PayTM before the Delhi High court that its customers alone have cumulatively lost nearly 10 Crores Rupees between the period from July 2019 to April 2020. It is further submitted by the PayTM that it is scrupulously following the guidelines issued by RBI in the interest of its customers.

26. The modus adopted by the fraudsters is like taking the customers to a malicious link or a phone number sent through SMS and when the customer dials the number or clicks the link so given, that would lead to

installation of some mirroring apps, malwares, and other modes which reveal sensitive information of the user. This enables the fraudsters to withdraw funds from the victim's bank account. Such kind of spying attacks have a deleterious effect upon the customers similar to the case in hand. It is also brought to the knowledge of the Court by the learned counsel for the petitioner that PayTM was banned from enrolling new customers. The RBI has taken action against PayTM under Sec.35-A of the Banking Regulation Act 1949 and directed PayTM to appoint an IT audit firm to conduct a comprehensive system audit of its IT system.

27. In fact, it is stated by the RBI that such an action has been taken based on certain materials connecting to supervising concerns observed by the bank itself. So the system audit is required for the IT system adopted by the 10th respondent, which is vulnerable to fraudulent activities. The petitioner is one among the several users and hence the 10th respondent is liable to make out the loss suffered by the petitioner. As it has been stated already that the complaint has been made by the customer to her banker, and the banker has kept in touch with PayTM, PayTM can not disown its

liability.

28. Since the RBI has been issuing directions to PayTM, as already cited, it is essential to issue one such direction to the 10th respondent to settle the loss suffered by the petitioner within the next two weeks. It is emphasised that the 10th respondent had failed to establish the liability on the part of the customer within 90 days as prescribed in the guidelines of the RBI, and hence the 10th respondent cannot state that the matter in issue involves a lot of facts to be gone into. The violations are crystal clear, and the 6th respondent has got the obligation to intervene when to the knowledge of the 6th respondent, the 10th respondent continues to violate the RBI guidelines and adopts an unfriendly attitude towards its users.

In the result, this Writ Petition is **allowed.** However, the relief is modified to the effect that the 6th respondent is directed to issue directions to the 10th respondent to make good the loss suffered by the petitioner without any other reduction, except the reduction of the amount, if any already reversed to the account of the petitioner in pursuant to the earlier order of this Court, within a period of two weeks. No cost. Consequently, the

miscellaneous petitions are closed.

28.04.2023

Index : Yes
Internet : Yes
Speaking:Yes
Neutral : Yes
jrs

To
1.The Commissioner of Police,
Office of the Commissioner of Police,
Vepery, Chennai-600 007.

3.The Deputy Commissioner,
K-4 Anna Nagar Police Station,
Anna Nagar, Chennai.

4. The Inspector of Police,
K-8 Police Station,
Arumbakkam, Chennai.

5.The Reserve Bank of India,
16, Rajaji Salai,
Fort Glacis, Chennai.

6.The City Union Bank,
Vigilance Department,
703, Anna Salai, Chennai.

7. The Assistant General Manager,
City Union Bank,
Vigilance Department,
24-B, Gandhi Nagar,

Kumbakonam 612 001.

8.The Manager,
City Union Bank,
Irungalur Branch,
Opposite SRM Campus,
Irungalur, Trichy.

9. PayTM Mobil Solutions Private Limited,
B-121, Sector 5, Noida-201301
India.

10.State Bank of India,
Rajaji Road,
Mannadi, Chennai Port Trust,
Chennai 600 001.

11.Fincare Small Finance Bank,
292, New No.116, Z Block II Avenue,
Beside Tower Metro Station,
Anna Nagar,
Chennai 600 040.

R.N.MANJULA, J.

jrs

Pre-delivery Order in
WP.No.6789 of 2021
and
WMP.Nos.7343 & 7345 of 2021

28.04.2023