Jus Corpus Law Journal
Open Access Law Journal – Copyright © 2022 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rishikesh Dave; Publisher – Ayush Pandey

Case Comment: HDFC Bank Limited v Jesna Jose

Rahul Srivastava[a]

[a]Campus Law Centre, University of Delhi, Delhi, India

Received 11 October 2022; *Accepted* 22 October 2022; *Published* 26 October 2022

INTRODUCTION

According to the RBI, over the last 7 years, India has lost INR 100 crore due to bank fraud every day. [1]The number of internet users has increased dramatically in recent years. Over 749 million people in India used the internet in 2020, accounting for over 41% of the country's humongous population[2]. Majority of the consumer services are now available online, allowing customers to access them from the convenience of their homes. Banking services are no exception. Every coin, however, has two faces. Although such a shift in the mode of conduction of such a necessary and demanding service online has offered huge benefits to the end users, at the same time it has offered an opportunity as an alternative tool for rogue elements to carry out their agenda by carrying out online banking frauds and thereby depriving the common man of his hard-earned money. In light of the above scenario, it becomes pertinent to fix the liabilities of the responsible

[1] 'India loses INR 100 cr to bank fraud every day over past seven years: RBI' (*Economic Times*, 29 March 2022) <https://economictimes.indiatimes.com/industry/banking/finance/banking/india-loses-rs-100-crore-to-bank-fraud-every-day-over-past-7-years-rbi/videoshow/90524910.cms> accessed 28 September 2022

[2] 'India' (*Data Common*) <https://datacommons.org/place/country/IND?utm_medium=explore&mprop=count&popt=Person&cpv=isInternetUser%2CTrue&hl=en> accessed 28 September 2022

entities (be it the bank, the financial intermediary involved, or the negligent customer herself) to reach a remedial course of action in such cases. The recent case discussed below tries to throw some light on the abovementioned issue.

FACTS IN THE PRESENT CASE

In this case, the Complainant (victim of the banking fraud) bought a pre-paid forex plus debit card having serial number 4123310000407245 having a capping of USD 10,000, coming from Opposing Party Number 2 (Manager of HDFC Bank Ltd.). Unauthorized transactions were carried out from the account attached to the above-mentioned card. According to the complainant, the records of the bank hinted at the fact that it was apprised of the fictitious transactions since the beginning of the fraud, despite this, the defendant took no action. The complainant victim also remarked that her initials did not match the initials on the charge forms. On complaint to the bank, the bank supplied records of SMS and email alerts to back its claim that the transactions were completed after validating the cardholder's credentials. Then after, the complainant made multiple requests to the concerned opponent bank, urging them to address her complaints and take appropriate action. The defendant, however, did not comply with the complainant's pleas.

The District Forum, as well as the State Consumer Disputes Redressal Commission (SCDRC), passed an order in favour of the complainant ordering the bank to pay the monetary damages back to the customer against which the present appeal was filed in the National Consumer Disputes Redressal Commission (NCDRC) at New by Section 21(b) of the 1986 Consumer Protection Act "*if it appears to the National Commission that such State Commission has exercised a jurisdiction not vested in it by law, or has failed to exercise a jurisdiction so vested, or has acted in the exercise of its jurisdiction illegally or with material irregularity, to call for the records and pass appropriate orders in any consumer dispute that is pending before or has been decided by any State Commission.*"

LEGAL ISSUE

- How should the liability be fixed in a case of online banking fraud?

- In the case of forgery/hacking or any other flaw in the electronic banking system's technical or security apparatus, what precautions can be taken by a customer to ensure that he gets his money back?

OBSERVATIONS OF NCDRC

- The panel highlighted that the applicant bank cannot evade its obligations to consumers by imposing arbitrary terms and conditions, and any such terms and conditions must b e by the guidelines established by the Reserve Bank of India (RBI), which is in charge of securing the banking systems and guaranteeing checks and balances within them.
- RBI circular of 6 July 2017 talks of "Dealing with Customer protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions"[3]
- Point 6 speaks for Zero Liability and Limited Liability.

GROUNDS FOR ZERO LIABILITY:

Contributory wrongdoing, carelessness, or weakness due to the bank's inefficiencies (regardless of whether the customer reports the transaction or not). If the problem is not with the consumer or the bank, but rather somewhere else in the system, it is a third-party breach, and the customer reports to the bank of the problem within three (3) working days after receiving notification from the bank about the unlawful transaction, he will have zero liability in such a case.

LIMITED LIABILITY

- The consumer is responsible for paying the full loss if they are careless and the incident is unreported. Any loss that occurs after reporting must be covered by the bank.
- The responsibility after 4–7 days shall be restricted to the transactional value as hereby specified; neither the bank nor the customer shall be liable.

[3] 'Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions' (*RBI)* <https://www.rbi.org.in/Scripts/BS_CircularIndexDisplay.aspx?Id=11040> accessed 28 September 2022

REPORTING TIMELINES

Post getting the communication from the concerned bank:

If reported under a time limit of three (3) days **– no liability**

Within 4-7 days – the transaction value or the amount of the maximum liability may range from 5000 INR to 25000 INR depending on the type of account opted for by the customer, whichever is lower.

Post seven (7) days – According to the Bank's policy. (Excluding the date of receiving the information)

Also, In *Punjab National Bank and Anr. v Leader Valves*,[4] while addressing the issue of a bank's accountability for unauthorized and fraudulent electronic banking transactions, the present Commission (NCDRC) made the following observations: "*Whether the Bank is liable for an unlawful transfer caused by an act of malfeasance by Bank officials or by an act of malfeasance by anybody else (apart from the Complainant/account-holder) is the first fundamental question that emerges. The response is clearly "yes" right away. If the Bank is the one maintaining the account, then the Bank is in charge of maintaining the account's security. Any systemic failure, whether caused by the functionaries' misconduct or that of any individual (other than the customer or account holder), is its duty, not the customers*."

JUDGEMENT

The national commission upheld the decisions made by the district and state fora of the commission, concluding that the challenged decision did not contain any flaws or violations that would warrant the appropriate intervention of the NCDRC justifiable according to Section 21(b) of the Consumer Protection Act, 1986. As a result, the revision petition was dismissed without a cost order.

[4] *Punjab National Bank & Anr v Leader Valves II* (2020) CPJ 92 (NC)

ANALYSIS

The present case sets an important precedent to ascertain the standards used to determine consumer culpability in the present situation of online banking in light of the sharpened focus on financial inclusion of the vulnerable section, presently out of the banking system and ensuring customer protection at the same time, as well as the recent surge in customer complaints relating to unauthorized transactions that result in unwarranted debits to their bank accounts. As was seen in the present case, the concerned banks deny their liability towards the customers in such cases of fraudulent transactions. This leaves the customer to look out for other remedial measures which add to the mental agony of the customer in addition to the already caused financial loss. The RBI has introduced a program known as the "Integrated Ombudsman Scheme" [5]to help alleviate customer complaints about services supplied by entities under its regulation in a timely and cost-effective way by Section 35A of the Banking Regulation Act.

As rightly held by the commission in this case, the customer cannot be held responsible for blatant violations of the RBI Guidelines and lack of adoption of requisite safety measures by the bank. If the customer has reported fraudulent transactions authenticated from his account without his wilful consent, then it becomes the duty of the bank to free the customer of any attached liability for loss of money on account of such transactions. The "Security and Risk Mitigation Measures for Electronic Payment Transaction" [6]were also introduced by the RBI, requiring banks to implement a minimum number of safeguards to lessen the impact of fraudulent attacks and stop/minimize damage. Apart from the above directives, various other measures have been taken by the banking sector Regulator to further complement the security of the banking infrastructure and the interests of the customers. Some of them are as follows –

Master Direction – KYC (Know Your Customer), 2016 updated 2018 - Streamlines Customer Identification Process. The later amendment spoke of the Video KYC.

[5] 'The Reserve Bank - Integrated Ombudsman Scheme, 2021' (*RBI*) <https://rbidocs.rbi.org.in/rdocs/content/pdfs/RBIOS2021_121121.pdf> accessed 28 September 2022
[6] 'Security and Risk Mitigation Measures for Electronic Payment Transactions' (*RBI*, 28 February 2013) <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=7874&Mode=0> accessed 28 September 2022

Where authorized persons conducting such KYC would have to collect the following from the customers –

- Capture video
- Pan
- Streaming from the authorized person
- Live Signature
- Geotagging for location

These steps ensure "Customer Due Diligence" and possibly can hold the customer not liable for "Deficiency in service" on the part of the bank.

- Proactive reporting can enable to start of the machinery against any possible attempt of online banking fraud.
- Secured connections, links, and Apps are crucial connections in online transactions. Hence, no security step is complete without taking into consideration their vulnerability to such attacks.
- Password changes regularly are an easy and effective step to create a new layer of protection every once in a while.
- Setting daily limits so that even if a fraudulent attack has been effected successfully the extent of damage can be limited and once the attempt has been recognized, the preventive and protective measures can be reined into.
- Enabling online alerts for all transactions /SMS/emails.

CONCLUSION

In the era of the internet wherein technology is changing so fast, no precaution can be ultimate. There is a constant updating in the strategies employed by fraudsters to breach the layers of security enabled to render as futile their attempts. But that cannot, and more importantly 'should not' feeble the willpower and commitment of the concerned authorities to secure the interests of the customers who have put in their faith and trust in the banking system and are

making their significant contribution to the economic development of the country by continuing to do so despite the above-discussed challenge.