RESEARCH QUESTION

"What legal steps can a person in India take after paying money to a fraudulent online seller or website, including cyber crime reporting under the IT Act, the national cybercrime portal and helpline 1930, *bank chargeback rights, and consumer forum remedies?"*

Legal Research Memo

⚠ Limited results: only 5 substantive cases were found for this query.

TL;DR

A victim of online cyber fraud must immediately report the transaction to the National Cyber Crime Reporting Portal (NCRP) or Helpline 1930 to trigger account freezing, and notify their bank to claim limited liability protection under RBI guidelines. While the High Court of Madras in *Dadha Pharma LLP v. Reserve Bank of India* (2025) confirmed that banks bear the burden of proving customer negligence to avoid zero-liability mandates, criminal prosecution under Section 66D of the IT Act and Section 420 of the IPC requires proving dishonest intent at the inception of the transaction rather than a mere civil breach of contract.

VERIFIED CASES	STATUTES	LATEST RULING
5	3	2025
5 *High Courts*		*Madras High Court*

CONTENTS

Prepared by Vitark AI · Strictly confidential · Verify citations before use

I. Detailed Analysis

KEY PRINCIPLES ESTABLISHED

01 Mandatory Registration of Cyber Complaints

Police authorities must register and investigate cybercrime complaints reported through the National Cyber Crime Reporting Portal (NCRP) irrespective of the monetary value of the fraud. This was clarified in *Megala Boominathan v. The Commissioner of Police* (2024), where the court rejected any minimum financial threshold (such as ₹5 Lakhs) for registering an FIR in online scams.

02 Interim Recovery of Frozen Scam Funds

Victims can petition the court for the release and recredit of cheated funds that have been successfully placed on hold or frozen in destination accounts during the investigation. As demonstrated in *Jai Pal v. State of NCT of Delhi* (2024), where siphoned funds are traced and frozen in an account, the victim may apply directly to the court for the release of the put-on-hold amounts.

03 Delineation of Fraud from Breach of Contract

Standard transaction disputes or non-delivery of goods by an online seller do not automatically constitute criminal cyber cheating unless fraudulent intent existed at the inception of the transaction. Under *Lalitkumar v. State of Maharashtra* (2025), a commercial dispute arising from non-delivery after payment is civil in nature, and criminal charges under Section 66D IT Act or Section 420 IPC will be quashed if there is no proof of initial deceptive intent.

04 Limitation on Bank Liability for Authenticated Credential Compromise

A bank cannot be held liable for losses resulting from fraudulent electronic transactions if the customer voluntarily shares sensitive credentials or downloads malicious apps that validate the transfer. In *Pallabh Bhowmick v. The Ombudsman, Reserve Bank of India* (2022), the Gauhati High Court held that when unauthorized transactions are completed using a customer's OTP, MPIN, and active credentials, and customer negligence is established, the bank is exonerated from liability.

HOW THE COURTS HAVE APPLIED THIS

HIGH COURT VARIATIONS

High Courts actively enforce the Reserve Bank of India's circulars regarding customer protection, emphasizing that the burden of proving customer negligence rests entirely on the bank. When third-party cyber breaches are established by police reports, the courts treat the transactions as disputed and order banks to restore the customer's funds, leaving the banks to seek civil remedies against the actual fraudsters.

II. Statutory Provisions

3 PROVISIONS

SECTION 66D, INFORMATION TECHNOLOGY ACT, 2000 — PUNISHMENT FOR CHEATING BY PERSONATION BY USING COMPUTER RESOURCE

This provision prescribes punishment for anyone who cheats by personation using any communication device or computer resource.

> "Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees." *Cited in*: Jai Pal v. State of NCT of Delhi

SECTION 66C, INFORMATION TECHNOLOGY ACT, 2000 — PUNISHMENT FOR IDENTITY THEFT

This section penalizes the fraudulent or dishonest use of another person's electronic signature, password, or unique identification features.

> "Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh." *Cited in*: (Not cited in results)

SECTION 420, INDIAN PENAL CODE, 1860 — CHEATING AND DISHONESTLY INDUCING DELIVERY OF PROPERTY

This provision establishes criminal liability and punishment for cheating that dishonestly induces a person to deliver any property.

> "Whoever cheats and thereby dishonestly induces the person deceived to deliver any property to any person, or to make, alter or destroy the whole or any part of a valuable security, or anything which is signed or sealed, and which is capable of being converted into a valuable security, shall be punished with imprisonment of either description for a term which may extend to seven years, and shall also be liable to fine." *Cited in*: Jai Pal v. State of NCT of Delhi, Lalitkumar v. State of Maharashtra, Megala Boominathan v. The Commissioner of Police

III. Cases Discussed

5 CASES · SUMMARY TABLE

#	CASE TITLE	COURT	YEAR	KEY HOLDING
01	*Dadha Pharma LLP v. Reserve Bank of India* HCMA012126512023	MADRAS HIGH COURT	2025	Exonerates customers under RBI zero-liability rules unless the bank proves customer negligence.
02	*Megala Boominathan v. The Commissioner of Police* HCMD010686862024	MADRAS HIGH COURT	2024	Directs police to register cyber fraud FIRs regardless of the monetary value lost.
03	*Pallabh Bhowmick v. The Ombudsman, Reserve Bank of India* GAHC010051612022	GAUHATI HIGH COURT	2022	Denies bank liability when unauthorized transfers result from customer-shared credentials or OTPs.
04	*Jai Pal v. State of NCT of Delhi* DLHC010737122024	HIGH COURT OF DELHI	2024	Permits victims to apply for the release of frozen fraudulent funds from destination accounts.
05	*Lalitkumar v. State of Maharashtra* HCBM030133362023	BOMBAY HIGH COURT	2025	Quashes criminal cyber charges for transaction failures lacking initial dishonest intent to cheat.

IV. Case Details

5 CASE FILES

01 Dadha Pharma LLP v. Reserve Bank of India

MADRAS HIGH COURT · 2025-06-12 · WP/413/2024

The petitioner filed a writ petition seeking a direction to their bank to recredit funds that were illegally siphoned from their current account. Although a police investigation confirmed the fraudulent transfer of funds, the bank failed to restore the money. The court examined RBI guidelines regarding customer liability in cases of unauthorized electronic transactions, noting that banks have a fiduciary duty to protect customer interests and bear liability for third-party breaches when notified promptly. Relying on precedents from other High Courts, the court emphasized that such unauthorized transactions are disputes that banks must address. The petition was filed to hold the bank accountable for the loss arising from the cyber fraud.

HELD The High Court held that a bank cannot debit or recover siphoned funds from a customer when the transaction is shown to be a disputed cyber transaction, unless the bank can unequivocally prove the customer's negligence in a civil court. Under applicable RBI guidelines, the law presumes the innocence of the customer in third-party cyber breaches. Thus, the bank's remedy is to restore the customer's funds and file a civil suit against the actual fraudster to recover the loss.

> “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 WPC 28823/2017 & 28824/2017 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.”

MADRAS HIGH COURT · 2025 | SOURCE HCMA012126512023

02 Megala Boominathan v. The Commissioner of Police

MADRAS HIGH COURT · 2024-07-29 · WP(MD)/15973/2024

The petitioner filed a writ petition seeking a direction to the police to act upon her complaint regarding a bank fraud where she lost over two lakh rupees. Although the police initially claimed they only register cases for fraud exceeding five lakhs, they subsequently registered an FIR after the court's intervention. The court emphasized that the police must act promptly on complaints without requiring judicial intervention for every case, noting that registration alone is insufficient without effective investigation and prosecution. The petition was allowed, and the police were directed to complete the investigation in a timely manner.

HELD The court established that cyber crime police cells must register all online fraud complaints on the National Cyber Crime Reporting Portal (NCRP) regardless of the financial loss involved. It flatly rejected the police's defense that FIRs are only registered for scams exceeding ₹5 Lakhs. Prompt registration of cyber complaints is mandatory to ensure timely investigation and tracing of defrauded money.

> "The Superintendent of Police has also stated that no oral or written order was passed to 4/9 https://www.mhc.tn.gov.in/judis WP(MD)No.15973 of 2024 register a case for a fraud of more than Rs.5 Lakhs alone. They are registering all the cyber crime complaints in National Cyber Crime Reporting Portal (NCRP), before assigning FIR or CSR to the complaint. He also states that they have registered 95,106 cyber complaints in the year 2023."

MADRAS HIGH COURT · 2024 | SOURCE HCMD010686862024

03 Pallabh Bhowmick v. The Ombudsman, Reserve Bank of India

GAUHATI HIGH COURT · 2022-09-30 · WP(C)/1900/2022

The petitioner, a bank customer, challenged the rejection of his complaint regarding unauthorized transactions totaling Rs. 94,204 from his savings account. The petitioner was defrauded by an individual posing as a brand representative, which led him to download a malicious mobile application, resulting in the unauthorized transfers. The bank and the Ombudsman denied liability, arguing that the transactions were validated by OTP and MPIN and occurred due to the customer's negligence in sharing his credentials.

HELD The High Court ruled that a bank cannot be held liable for losses suffered by a customer due to an unauthorized transaction if the bank cogently establishes customer negligence. While banks bear the primary duty of maintaining robust cyber security, sharing sensitive credentials (such as OTP, password, or MPIN) or downloading malicious apps that compromise credentials shifts the loss entirely to the customer until the fraud is formally reported.

> "It is no doubt correct that if a customer is negligent in handling his or her account and discloses sensitive information such as, password, OTP, MPIN, Card Number etc. resulting into fraudulent transaction, the Bank cannot be held liable for loss, if any suffered by the customer. However, in such cases, negligence on the part of the customers must be cogently established by the Bank by bringing reliable materials on record. The Banks cannot absolve themselves of the liability towards losses suffered by the customers on account of unauthorized electronic transactions based on perceived negligence of the customers."

GAUHATI HIGH COURT · 2022 | SOURCE GAHC010051612022

04 Jai Pal v. State of NCT of Delhi

HIGH COURT OF DELHI · 2024-12-02 · BAIL APPLN./3926/2024

The applicant sought bail in connection with an FIR involving charges of cheating and cyber fraud. The complainant alleged being lured into a fraudulent WhatsApp trading scheme, resulting in significant financial loss. While the prosecution argued that the applicant operated the bank account used to receive the cheated funds, the applicant contended that his account was misused by a co-accused. The court noted that the investigation had concluded and a chargesheet had been filed. Observing that the trial would likely take considerable time, the court granted the bail application subject to specific conditions, including a personal bond and travel restrictions, emphasizing that the merits of the case would be determined at trial.

HELD The court acknowledged that where cyber fraud has taken place, money siphoned from the victim is typically traced and placed on hold in the suspect's bank account. The victim can move an application before the court for the release and restoration of these frozen funds while the trial proceeds. The court granted bail to the applicant whose account was used, noting that the siphoned sum had been successfully frozen.

> "On being asked, it is pointed out that a total sum of ₹15,00,000/- has already been put on hold in the bank account of the applicant and the complainant has moved an application for release of the said amount."

HIGH COURT OF DELHI · 2024 | SOURCE DLHC010737122024

05 Lalitkumar v. State of Maharashtra

BOMBAY HIGH COURT · 2025-04-03 · APPLN/1238/2023

The applicant sought to quash an FIR and subsequent criminal proceedings involving allegations of cheating and identity theft under the Indian Penal Code and the Information Technology Act. The dispute arose from an alleged breach of an oral contract for the supply of fertilizer, where the complainant claimed non-delivery of goods despite payment.

HELD The High Court held that a mere contractual failure to deliver goods after receiving payment does not constitute criminal cheating under Section 420 IPC or computer-based personation under Section 66D of the IT Act. For cybercrime penal sections to apply, there must be clear evidence of deceptive intent from the very beginning of the transaction, or evidence of identity theft or impersonation through computer resources. Otherwise, the dispute is purely civil.

> "Thus, taking into consideration the FIR and the contents of the charge-sheet, it can be seen that a civil transaction is given a criminal colour i.e. for alleged contract, when respondent No.2 had paid the amount for the goods ordered, the goods are not delivered. There is nothing in the FIR to indicate that the accused had intention to cheat since beginning."

BOMBAY HIGH COURT · 2025 | SOURCE HCBM030133362023

DISCLAIMER