

BANKS' LIABILITY FOR UNAUTHORIZED ELECTRONIC TRANSACTIONS IN INDIA: A STUDY OF CUSTOMER PROTECTION IN DIGITAL BANKING

by

P Naveen Kumar

B.B.A.LL.B. (Hons.)

School of National Security and Law, Rashtriya Raksha University, Gandhinagar, Gujarat, India

Abstract

India has made significant shifts towards digital banking, using UPI, mobile banking, cards and net banking to make payments faster and cheaper. However, as a result of these developments, the risk of banking fraud has shifted from the branch counter to the customer's phone. In cases where a customer's bank account is debited without her authority, the law in India attempts to answer the question as to who should bear that loss – the bank or the customer. This paper discusses the law on this issue in India. It begins by discussing the relationship between the banker and the customer, then analyses the Reserve Bank of India's circular of 6 July 2017 on limiting the liability of customers. It also analyses the approach of the courts; in particular the Gauhati High Court and the Supreme Court in *State Bank of India v. Pallabh Bhowmick*. Furthermore, the paper investigates the remedies available to customers under the Consumer Protection Act 2019, the Information Technology Act 2000 and the RBI Integrated Ombudsman Scheme. Additionally, the paper evaluates the RBI's 2026 amendment directions on digital fraud compensation for small values. The Indian law on this issue is also compared to the laws of the United Kingdom, the United States and Singapore. The paper argues that the 2017 RBI framework is sound in principle, but could be improved with more specific standards, better enforcement and changes to accommodate socially engineered fraud. Finally, specific suggestions are made for the reform of the digital fraud compensation framework.

Keywords: unauthorized electronic transactions; banks' liability; zero liability; RBI circular 2017; digital banking; customer protection; UPI fraud; burden of proof.

Introduction

Digital payments are the ordinary way that money moves in India today. From the tea stall to the salary transfers to the shopping carts, digital payments in some form flow through every transaction. The infrastructure that has given so many Indians access to the financial system has also allowed for a growing volume of financial fraud. Some of the frauds reported include phishing links, SIM swaps, fake customer care numbers, remote access applications, compromised merchant sites, and frauds that target the customer directly. The Reserve Bank of India has noted that small-value frauds make up a very large share of the number of fraud cases reported in the country, even if those small value frauds account for a smaller share of the total value lost in those cases (RBI, Statement on Developmental and Regulatory Policies, 6 February 2026).

For the victim of an unauthorised electronic transaction, the loss is rarely just financial. The victim must prove that she did not authorise the transaction against an institution that has the logs, the authentication records and the technical expertise to prove that. The traditional banking contract was never designed to accommodate this imbalance. A cheque carries a signature that the bank can compare against, and the law of forged cheques developed around that concept. Electronic debits carry no signature, only a credential that the bank asserts were used by the customer.

The research question for this study concerns how Indian law allocates liability between the banks and the customers for unauthorised electronic transactions, and how effectively that allocation protects the customers from losses due to such unauthorised transactions.

The paper has four objectives: (i) to explain the legal relationship between banker and customer in the digital setting; (ii) to analyse the RBI's limited-liability framework and the way courts apply it; (iii) to assess the statutory and quasi-judicial remedies actually open to a defrauded customer; and (iv) to evaluate recent reforms and propose improvements.

The research follows a doctrinal approach. The research bases its findings on primary documents which include statutes and RBI circulars and directions and judicial decisions and secondary materials that consist of commentary and regulator statements. The research compares three legal

systems from different territories but it does not analyse how their respective frameworks generate specific results. The research paper focuses on fraud cases which impact corporate customers but it does not investigate loan-related mis-selling practices except for cases that matter. The law exists as it did in October 2026 because the regulatory position continues to change.

The Banker-Customer Relationship and the Foundation of Liability

The starting point of English and Indian banking law is that the relationship between banker and customer is, in its core, one of debtor and creditor. In *Foley v. Hill* (1848) 2 HL Cas 28, the House of Lords held that money paid into a bank becomes the bank's property, and the bank owes a debt to the customer. *Joachimson v. Swiss Bank Corporation* [1921] added that the bank must repay on demand, at the branch where the account is kept, and that the customer owes a duty of care in drawing cheques. Indian courts have followed this approach, and it was affirmed in the context of cyber fraud when the Supreme Court's decision in *Pallabh Bhowmick* was read as treating the relationship as debtor and creditor rather than trusteeship (see Verlekar, 2025).

Some consequences follow from these points. The bank only pays on the customer's mandate. If the bank debits the account without the customer's authority, it is not a payment of the customer's debt. Secondly, the bank owes an implied duty of reasonable skill and care to the customer. In *Barclays Bank v. Quincecare* [1992] 4 All ER 363, the court held that the bank owes a duty to the customer to not execute an order that the bank has reasonable grounds to believe is an attempt to misappropriate the customer's funds. The Indian courts have not adopted this duty, but the Supreme Court's directive to banks to use the best technology available to prevent fraudulent transactions expresses the same idea. The customer also owes some duties to the bank. In *Tai Hing Cotton Mill v. Liu Chong Hing Bank* [1986] AC 80, the court held that the customer is required to take reasonable care in the way she draws cheques and to inform the bank of any forgeries. However, she has no duty to run her audit of the bank's systems. These duties map onto the modern framework where the customer must guard her credentials and report any fraudulent transactions as quickly as possible, and the bank must provide a secure system for its customers.

The duties in the digital setting are different from the duties in the physical world. For instance, authentication in electronic banking requires the customer to provide a PIN or password (something the customer knows) or a registered mobile number or card (something the customer

has). The bank claims that once someone is authenticated, they are authorised to make transactions on the customer's account. However, authentication does not prove that the account holder actually provided the credentials. This gap between authentication and authorisation is the major problem of the field.

Analysis of Roopam Kumar vs SBI cards & payment service

The genesis of the present dispute traces back to December 2017 when Roopam Kumar, a resident of Mohali, was approached by an agent of SBI Cards & Payment Services Private Limited. The agent, employing persuasive tactics, induced the complainant to obtain a credit card and obtained her signature on certain blank forms. Subsequently, the banking institution issued a credit card bearing the number ending in 6048 to the complainant.

The tranquillity of ordinary financial dealings was disrupted in 2017, when the complainant received two suspicious one-time password messages on her mobile device. The first message at 11:02 AM, indicated a transaction of Rs. 10,000 at Airtel-Money using her SBI Card. Within a minute, at 11:03 AM, another message arrived notifying a second transaction of Rs. 999 at the same merchant. Both messages explicitly warned the recipient not to share the OTP with anyone, raising immediate red flags regarding the legitimacy of these transactions.

The complainant was shocked by these notifications for transactions and thus immediately contacted the opposite party to report the suspicious activity. Her swift action resulted in the banking institution blocking the credit card on the same day, merely minutes after the fraudulent transactions occurred. The bank registered her complaint, formally acknowledging receipt of her grievance.¹

Legal Framework and Regulatory Provisions

The Commission's analysis extensively relied upon the Reserve Bank of India's Circular No. RBI/2017-18/15 DBR.No. Leg.BC.78/09.07.005/2017-18 titled "Customer Protection – Limiting Liability of Customers in Unauthorized Electronic Banking Transactions." This comprehensive regulatory framework establishes clear guidelines for determining customer liability in cases of unauthorized electronic banking transactions.

The circular introduces the concept of zero liability for customers in specific circumstances. A customer becomes entitled to zero liability when unauthorized transactions occur due to

¹ Ritika Dedhia, *Bank's Liability for Unauthorized Electronic Transactions: Analysis of Roopam Kumar v. SBI Cards & Payment Services*, <https://www.indialaw.in/blog/consumer/unauthorized-electronic-transactions/>.

contributory fraud, negligence, or deficiency on the part of the bank. Additionally, zero liability applies in cases of third-party breaches where the deficiency lies neither with the bank nor with the customer, provided the customer notifies the bank within three working days of receiving communication regarding the unauthorized transaction. The regulatory framework imposes stringent obligations upon banking institutions. Upon notification by the customer, the bank must credit the amount involved in the unauthorized transaction to the customer's account within ten working days through a shadow reversal mechanism. This obligation exists independent of any insurance claim settlement and does not require the bank to await such proceedings.

Furthermore, the circular mandates that complaints must be resolved within a timeframe specified in the bank's board-approved policy, not exceeding ninety days from the date of receipt of the complaint. If the bank fails to resolve the complaint within this ninety-day period, compensation as prescribed in the circular must be paid to the customer. Critically, the circular places the burden of proving customer liability squarely upon the banking institution. This reversal of the traditional burden of proof reflects the regulatory recognition of the superior position of banks in electronic transaction ecosystems and their corresponding responsibility to maintain strong security systems.

Judicial Precedents and Legal Reasoning

The Commission fortified its decision by relying upon several authoritative precedents that addressed similar issues. The Bombay High Court's Division Bench, comprising Justice Girish Kulkarni and Justice Firdosh Pooniwalla, in the matter of Jaiprakash Kulkarni and Pharma Search Ayurveda Pvt. Ltd., had applied the 2017 RBI Circular and held that customers bear zero liability when unauthorized transactions occur due to third-party breaches where the deficiency lies not with the bank or customer but somewhere in the system. In that case, the High Court directed Bank of Baroda to refund Rs. 76 lakh that had been fraudulently debited from a company's bank account.²

Final Determination and Relief Granted

Based on its comprehensive analysis, the Commission partly allowed the consumer complaint and issued specific directions to the opposite party. The bank was directed to refund the amount

² Ritika Dedhia, *Bank's Liability for Unauthorized Electronic Transactions: Analysis of Roopam Kumar v. SBI Cards & Payment Services*, <https://www.indialaw.in/blog/consumer/unauthorized-electronic-transactions/>.

of Rs. 35,594 to the complainant, along with interest at the rate of nine percent per annum calculated from the date of its deposit until the date of actual realization.

The Commission directed the banking institution to remove the complainant's name from the defaulter list maintained by CIBIL and other credit information bureaus. This direction was crucial for restoring the complainant's creditworthiness and preventing future financial disabilities arising from the wrongful reporting.

Recognizing the prolonged harassment, mental agony, and litigation expenses borne by the complainant over nearly five years of pursuing her rightful claim, the Commission awarded compensation of Rs. 10,000. It was both recognition of the complainant's suffering and a deterrent against similar conduct by banking institutions. The Commission stipulated that compliance with its order must be completed within forty-five days from the date of receipt of the certified copy of the order, ensuring timely relief to the aggrieved consumer.

Implications and Conclusions

This judgment carries significant implications for the banking sector and consumer protection jurisprudence. It reaffirms that banking institutions cannot adopt a cavalier attitude toward customer grievances, particularly concerning unauthorized electronic transactions. The strict liability imposed upon banks reflects their superior position in the financial ecosystem and their corresponding duty to maintain strong security systems and grievance redressal mechanisms.

The decision reinforces that regulatory circulars issued by the Reserve Bank of India are not merely advisory but constitute binding obligations upon banking institutions. Non-compliance with such regulatory frameworks constitutes deficiency in service actionable under consumer protection laws. The reversal of the burden of proof, placing it upon banks rather than customers, recognizes the inherent information asymmetry and technical complexities involved in electronic banking fraud.

The case also highlights the importance of documentary evidence in consumer disputes. This decision represents the consumer forum's commitment to protecting vulnerable consumers against institutional high-handedness and ensuring that banking institutions honor both their regulatory obligations and their duties toward customers who repose faith in their services.³

³ Ritika Dedhia and Tanvi Dalvi, <https://www.indialaw.in/blog/consumer/unauthorized-electronic-transactions/>.

Exploring safeguards in digital payments to curb frauds

Regulatory measures to secure digital payments

- Over the years, the Reserve Bank has introduced several measures to strengthen the safety and resilience of digital payments. Two-factor authentication was mandated in digital payment transactions. Storage of actual card data by any entity in the payment chain, other than the card issuer, was sought to be restricted through device tokenisation (2019) and card-on-file tokenisation (2021). Customer induced controls in cards were mandated in 2020 thereby empowering cardholders to switch on / off and set / modify transaction limits (within the overall card limit, if any, set by the issuer) for all types of transactions – domestic and international, at online transactions/contactless transactions, etc.
- Instructions regarding digital payment system controls for banks (2021) and non-bank PSOs (2024) were issued covering aspects such governance mechanisms for identification, assessment, monitoring and management of information systems and cyber security risks, along with baseline security measures for ensuring system resilience as well as for safe and secure digital payment transactions. In 2025, the Bank issued a principle-based framework for authentication of digital payment transactions to encourage introduction of new factors of authentication by leveraging upon technological advancements and to enable issuers to adopt additional risk-based checks beyond the minimum two-factor authentication based on fraud risk perception of the underlying transaction.
- The customer's liability is limited in case of unauthorised electronic banking transactions as mentioned in instructions issued in 2016.
- RBI has also issued directions to various system participants to utilise the Mobile Number Revocation List (MNRL) available on the Digital Intelligence Platform (DIP) developed by Department of Telecommunications (DoT), to monitor and clean their customer database. Telecom Regulatory Authority of India (TRAI) has issued directions to use phone numbers that begin with the '1600xx' series for calling customers regarding transactions or service-related provisions. Further, any marketing or promotional calls should be made from numbers in '1400xx' series. These measures aim to help consumers distinguish between legitimate calls and potential scam attempts made by fraudsters.

- Indian Cybercrime Coordination Centre (I4C) has issued a Standard Operating Procedure to deal with complaints lodged with National Cybercrime Reporting Portal (NCRP).
- In 2024, Reserve Bank's wholly owned subsidiary - Reserve Bank Innovation Hub (RBIH) has built Mulehunter.AI to enable quick and effective detection of mule bank accounts by the banks. The Reserve Bank is also presently working with RBIH to set-up prototype of a Digital Payment Intelligence Platform (DPIP) by harnessing advanced technologies (AI/ML) to mitigate payment fraud risks. To a remitting bank, the platform is envisaged to provide information about the beneficiary's profile through a risk score generated on a real-time, transaction-by-transaction basis, even before the transaction is executed.⁴

The Legal and Regulatory Framework

The Banking Regulation Act, the RBI Act and the Payment and Settlement Systems Act.

The Reserve Bank of India obtains its banking operational authority from the Banking Regulation Act 1949 together with the Reserve Bank of India Act 1934. The Payment and Settlement Systems Act 2007 serves as the regulatory framework for electronic payment systems which enables the RBI to grant operational approval and establishes operational criteria and provides enforcement authority against system participants. None of these statutes sets out a rule on who bears the loss from an unauthorised electronic debit. The rule therefore lies in subordinate regulation and in general contract and consumer law.

The core instrument consists of the RBI circular which protects customers through its rules about unauthorized electronic banking transaction liability (DBR.No. Leg.BC.78/09.07.005/2017-18, 6 July 2017). The document presents multiple essential components which form its main structure. Preventive duties. Banks need to develop systems which will detect fraud attempts while blocking their occurrence and they must enable customers to receive SMS transaction alerts through their electronic banking system. The organization needs to operate a 24-hour reporting service which accepts unauthorized transaction claims while they provide initial complaint numbers when they receive each report. Banks need to explain every customer right and duty which includes their responsibility to pay for any losses that occur.

⁴ Discussion Paper - Exploring Safeguards in Digital Payments to Curb Frauds, <https://www.rbi.org.in/Scripts/PublicationsView.aspx?id=23810>.

Zero liability (clause 6). The customer has no liability where the unauthorised transaction results from (a) contributory fraud, negligence or deficiency on the part of the bank, whether or not the customer reports it, or (b) a third-party breach where the deficiency lies neither with the bank nor with the customer, and the customer reports within three working days of receiving the bank's communication.

Limited liability (clause 7). The customer must pay all losses which occur before she contacts the bank when she shares her payment credentials but the bank will handle all losses that happen after she contacts them. The customer needs to pay the entire transaction amount or reach the established limit which applies to the situation when she reports the loss to the bank between four and seven working days after the third-party breach occurred. The banking system establishes ₹5,000 as the maximum balance for basic savings accounts while it sets ₹10,000 and ₹25,000 for other current accounts and higher-limit cards. The bank's board-approved policy will determine responsibility when someone files a report which exceeds seven business days for processing.

Reversal and burden of proof (clauses 8 and 9). The bank must credit the amount involved (a shadow reversal) within ten working days of the customer's notification, without waiting for the end of the investigation, and must resolve the complaint within ninety days. The burden of proving customer liability rests on the bank. The circular in design represents a system which distributes risks through a graded allocation system. The level of liability depends on both fault and speed because innocent customers who act quickly receive no responsibility but those who delay become partially responsible and negligent customers must bear complete responsibility. The system requires the data holder to prove their information because it acknowledges that different parties possess varying levels of knowledge

Related RBI instruments

The RBI's Master Direction on Digital Payment Security Controls (2021) requires regulated entities to adopt a governance framework, authentication controls and monitoring for internet, mobile and card channels. The RBI's framework on turn-around time (TAT) for failed transactions, issued in 2019, requires automatic reversal within prescribed timelines and compensation of ₹100 for delay beyond the limit. These instruments set a baseline of security and service from which a deficiency can be inferred when fraud occurs.

RBI 2017 circular: foundation of bank liability

With the release of its 2017 Circular under Section 35A of the Banking Regulation Act, 1949, the Reserve Bank of India created a framework for ensuring accountability in digital banking. The circular reallocates risk by placing the burden of proof on the banks to prove the negligence of their customers before denying relief to those customers..

The circular sets out a proper procedure for customer liability as follows:

- In cases where the customer has no liability (zero liability), the bank shall have full liability. It shall occur when the customer is not responsible for the unauthorized transaction and when it is due to bank negligence, such as system vulnerabilities, internal bank fraud, or inadequate security. However, these zero liabilities of customers will also apply to cases involving unauthorized transactions due to a third-party breach, such as identity theft, unauthorized electronic transactions, etc., provided that the customer has not been party to the fraud and has reported the same to the bank within the prescribed time frame of 3 working days of the transaction.
- In cases where the customer has limited liability to the bank, the customer will have only limited liability to the bank for unauthorized electronic banking transactions when the customer delays in reporting the transaction to the bank, and the delay is within 4 to 7 working days. Thus, customers' liability will be limited to the amounts set by the RBI and the bank's policy.
- Lastly, in cases where customers are fully liable to the bank for unauthorized electronic banking transactions, their liability is voluntarily shared due to their negligence, which involves disclosing sensitive information such as OTPs, PINS, and passwords.

It also mandates that banks provide provisional credit within the prescribed time frame and resolve all complaints within 90 days. Secondly, it should place the burden of proof on banks to showcase customer negligence. It represents the shift towards enhancing bank accountability for digital transactions.⁵

⁵ Vidhi Dobhal & Spriha Bisht, Liability of Banks in Online Banking Fraud: Need for a Stronger Consumer Protection in India, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=7280999.

Judicial Approach to Banks' Liability

State Bank of India v. Pallabh Bhowmick

One of the leading modern cases on the subject is *State Bank of India v. Pallabh Bhowmick*. The customer in this case attempted to return an item that was bought online. However, he was tricked into installing an application on his phone by a purported customer service agent. On the 18th of October, 2021, a total of three unauthorised transactions took place from the customer's account, ₹94,204.80. The customer reported the transactions to the bank on the subsequent working day. The bank responded by blocking the customer's debit card, but refused to reimburse the customer as they claimed that the customer had shared the OTPs and M-Pin with the third party. The Gauhati High Court single judge held the bank liable for the transactions. The Division Bench dismissed the bank's writ appeal on the 13th of September, 2024 (WA 364/2022). The Division Bench relied on the 2017 circular relating to zero liability and held that the bank could not attribute liability to the customer without proving negligence on the part of the customer. The bank failed to show that the customer was complicit in the transactions or that the bank had exercised due diligence in attempting to prevent the transactions. The Supreme Court of India, through a bench of Justices Pardiwala and Mahadevan, dismissed the bank's special leave petition on the 3rd of January, 2025 (SLP (C) No. 30677/2024). The Supreme Court agreed with the findings of the Division Bench that the transactions were reported within the period required for zero liability. The Court also found that the bank had the technological ability to detect and prevent such transactions. Furthermore, the Court stated that customers should remain extremely vigilant in their banking transactions, and never share their OTPs with third parties.

The limits of the precedent

Pallabh Bhowmick is an important case, but its importance should not be overstated. The Supreme Court disposed of the matter by a short order at the admission stage of the case, and so it is not a fully reasoned judgment that lays down a general rule for every case of socially engineered fraud. Essentially, the Supreme Court has endorsed the High Court's reading of the circular on the facts of that case, where there was prompt reporting of the fraud and the bank had not been shown to be negligent. A subsequent decision of the Allahabad High Court in a case involving Bank of Baroda also treated the decision in *Pallabh Bhowmick* as being confined to its

facts. The court confirmed that the burden of proof lies on the bank but held that the bank had discharged its burden of proof through the evidence that it presented. Accordingly, the court refused to grant any relief to the customer. The Bombay High Court has also considered the 2017 circular in the context of proceedings before the Banking Ombudsman (Jaiprakash Kulkarni v. Banking Ombudsman, 2024 SCC OnLine Bom 1666).

The law that emerges is a balance. The bank must prove negligence with evidence, but if it produces credible technical evidence, such as logs showing that the customer herself added the beneficiary or entered the OTP, courts will uphold the bank. In the absence of such evidence, the customer prevails. This makes the quality of the bank's evidence, rather than a presumption either way, decisive.

Remedies Available to a Defrauded Customer

Internal grievance redressal and the RBI Integrated Ombudsman Scheme

Customers can first lodge a complaint with the bank, which will respond and reverse the transactions according to the circular. If the bank does not resolve the complaint within 30 days or rejects the complaint, customers can approach the RBI Ombudsman under the Reserve Bank – Integrated Ombudsman Scheme 2021. The RBI removed the earlier banking, NBFC and digital transactions ombudsman schemes and introduced a single forum with a single point of entry for all banking and financial complaints. The Ombudsman can award customers the amount lost, compensation for the loss of time, expenses and for the harassment caused. The scheme was revised in 2026 to broaden the powers of the Ombudsman and to increase the ceiling of the compensation for mental agony suffered by the complainants. However, the report of these revised figures is not relied upon in this paper; readers should verify the figures from the official scheme before citing them. The RBI Ombudsman route is inexpensive and does not require a lawyer, making it the most realistic route for small claims.

Consumer Protection Act 2019

Under section 2(42) of the Consumer Protection Act 2019, a bank customer is a 'consumer' and banking is a 'service'. Any failure of the bank to secure the account against unauthorised debits or failure of the bank to reverse a debit that is required to be reversed by the circular can be pleaded as a 'deficiency in service' under section 2(11). Complaints can be made to the District, State or National Commission depending upon the value of the consideration paid by the consumer (₹50

lakh, ₹2 crore, above ₹2 crore respectively as per the 2021 rules). The Commissions have awarded the disputed sum, interest and compensation for mental harassment to the consumers. Thus, the Consumer Protection Act provides a court-like remedy that is cheaper and faster than a civil suit.

The Information Technology Act 2000 and the Digital Personal Data Protection Act 2023

Section 43A of the Information Technology Act makes a body corporate liable to pay compensation for negligence in implementing reasonable security practices. Financial information is included within the definition of sensitive personal data in the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011. Section 43 of the IT Act gives civil liability for accessing a computer system without permission. Sections 66C and 66D make identity theft and cheating through personation using a computer resource punishable offence. An adjudicating officer appointed under section 46 can award compensation. Section 43A of the IT Act has seldom been used against banks. The Digital Personal Data Protection Act 2023 requires data fiduciaries to adopt reasonable security safeguards to prevent personal data breaches. It provides for penalties for failure to adopt the safeguards. As this Act comes into force in stages, the liability of banks for data breaches will become clearer. However, this Act indicates that the standard of care that banks must exercise for the security of their customers' data is increasing.

The 2026 Reforms: From Limiting Liability to Compensating Loss

In the Statement on Developmental and Regulatory Policies from the Reserve Bank of India dated 6 February 2026, a framework was announced to compensate customers for small-value digital frauds. A draft of the amendment was published on 6 March 2026. The final Reserve Bank of India (Commercial Banks – Responsible Business Conduct) Third Amendment Directions, 2026 were issued on 24 June 2026 and are due to take effect on 1 January 2027, which is six months later than the draft proposed (Money life, 25 June 2026).

- The main features of the final directions are as follows: A customer that suffers a fraud loss of up to ₹50,000 and ₹25,000 may receive compensation of 85 per cent of the net loss.

- This compensation may only be claimed once in the lifetime of a customer. The cost of the compensation is to be shared between the Reserve Bank of India, the customer's bank, and the beneficiary bank, with the RBI bearing the largest share of the cost.
- The fraud must be reported within five days in order to qualify for compensation.
- The draft would have allowed for compensation for later reports of the fraud. The final text drops that and provides that, in cases where there is a breach by a third party and reported after five days, the liability will be as per the policy of the bank.
- The directions are also reported to speed up the acknowledgement and resolution of complaints and to define a standard dispute process with escalation to the Ombudsman.

The updates bring three essential elements into the existing system. The policy acknowledges that victims who authorized payments through deception need protection because they do not qualify for zero-liability coverage. The beneficiary bank supports this approach because they understand mule accounts function as a criminal system. The funding source operates independently from bank fault assessment requirements.

There are, however, limits. The ₹25,000 cap and the once-in-a-lifetime rule leave larger and repeat victims outside the scheme. The compensation exists as a separate benefit which does not provide full refund rights to customers who did not cause their losses. Banks might use the "negligence" classification to direct claims toward the capped scheme instead of giving customers their full money back. The five-day reporting requirement may also exclude victims who discover fraud late. The 2017 circular will stay in power until the new directions become effective.

Comparative Perspective

- **United Kingdom:** The Payment Services Regulations 2017 demand payment service providers to return unauthorized payments while providers must establish that payments received proper authentication and customers showed complete negligence or fraudulent conduct. The Payment Systems Regulator rules starting from October 2024 mandate firms to repay authorized push payment (APP) scam victims up to £85,000 per claim which both sending and receiving firms must equally fund. The document presents the most similar material to the 2026 Indian reforms which expand protection for victims who authorized payments through deceptive means.

- **United States:** Regulation E under the Electronic Fund Transfer Act protects consumers from unauthorized transfers by limiting their financial responsibility to \$50 when they report the loss or theft of their access device within two business days of discovering the loss. The consumer must report the loss within two business days to limit their liability to \$50 but their responsibility increases to \$500 after two days until the sixty-day limit for reporting passes. The tiered structure resembles India's 2017 scheme, and both place the burden on the institution.
- **In Singapore:** The Shared Responsibility Framework has been implemented in December 2024. The framework allocates the responsibility for phishing scams to the banks, telecommunications operators and the consumers according to the anti-scam duties performed by each of these parties. The main contribution of this framework is the recognition of the loss in phishing scams as a systemic loss involving several actors, rather than just the bank and the customer.

India's approach to managing phishing scams compares well with Singapore in the burden of proof and the reversal timelines for the scams. However, India lags behind Singapore in three points. India does not have a statutory basis for its approach to phishing scams. The compensation that is provided for socially engineered fraud is capped and only provided once. Finally, India does not extend the responsibility for phishing scams to other actors in the chain of the scam, such as the telecommunications operators and the platform on which the scams are performed.

Critical Analysis and Gaps

1. **Regulation through Circular:** The rights of the customers is established through a circular of the RBI and not through any statute of law passed by the Parliament. Though the courts have enforced the circular, its legal status has been challenged in some cases. The circular can also be amended by the RBI without debate in the Parliament. Having a statutory right for the customers would provide a more secure foundation for the rights of the customers and make enforcement of these rights more predictable.
2. **Vague Standards of Negligence:** The circular does not provide any definition of negligence on the part of the customer. Banks treat any instance of the customers disclosing their credentials to be negligent on the part of the customer. The burden is placed on the customers to prove that they were tricked into disclosing their credentials.

Having a defined criteria for negligence would create more consistency in the outcomes of these cases.

3. **Evidence Asymmetry:** The banks hold all of the logs, device data and authentication data for the transactions initiated by the customers. The burden of proof is on the banks to prove their case. However, the customers have little to no access to the evidence needed to prove their case. There should be a clear right for the customers to obtain the transaction logs of the banks on request together with an adverse inference where the bank does not produce them would make the burden meaningful
4. **Non-compliance with timelines:** Customers report banks fail to provide shadow reversal within ten business days because they extend the investigation process. The circular's timelines are of little value without penalties.
5. **Social engineering:** The 2017 framework assumed that fraud occurred through a breach by a third party. The system encounters difficulties because more scammers have started using fraudulent payment methods which let customers authorize payments under false pretences. The 2026 compensation scheme addresses this only in part.
6. **Weak transaction-monitoring duty:** Banks must track their operations through monitoring systems yet no established criteria exist to determine what constitutes an adequate detection mechanism. The Supreme Court established an elevated requirement through its Pallabh Bhowmick comments yet it did not establish this as an official evaluation standard. The adoption of delayed credit for new payees and velocity limits and friction on high-risk transactions varies across different organizations.
7. **Customer awareness:** Many customers do not know that the three-day reporting window is critical. Reporting late is the commonest reason for lost protection.

Suggestions

1. **Statutory codification:** The main framework of the limited-liability system should become statutory law through either independent legislation or Banking Regulation Act and Payment and Settlement Systems Act amendments which require banks to prove their claims.
2. **Define negligence:** The RBI needs to establish example standards which demonstrate customer negligence and bank deficiency because deceptive disclosure does not always indicate negligence when banks miss detecting suspicious transactions.

3. **Mandatory disclosure of evidence:** Banks must deliver their customers the exact authentication records and logs which they used to deny claims within a specified time frame while courts will apply adverse inference to banks which fail to provide these documents.
4. **Penalty for delayed reversal:** The company should pay customers an immediate penalty which matches the current TAT compensation when the organization fails to deliver shadow credit within the established ten working day period.
5. **Shared responsibility:** The Singapore model requires telecom operators and payment apps and receiving banks to assume responsibility for mule accounts which they should manage effectively.
6. **Time-bound freezing:** There should be a statutory mechanism that allows the account to be frozen immediately upon receipt of a credible report, with appropriate judicial review to protect innocent account holders' rights.
7. Raise the compensation ceiling and review the lifetime limit once data on the scheme becomes available, and ensure that it does not substitute for the full zero-liability right.
8. Customer education. Banks should include prominent warnings and reporting information with each alert, and the RBI should track and publish complaint-resolution data by bank.

Conclusion

Indian law with regard to unauthorised electronic transactions is based on a sound principle. The party that designs, operates and profits from the payment system is in a better position to prevent frauds and absorb losses than the customer. The 2017 circular of the Reserve Bank of India gives effect to this principle. In the case of *State Bank of India v. Pallabh Bhowmick*, the courts enforced this principle. However, the decision in this case also shows the limits of this principle. The 2026 reforms to the law on unauthorised electronic transactions are a shift from the idea of limiting the liability of customers towards compensating them for the losses that they suffer. These reforms are a response to the reality of socially engineered frauds. However, these reforms are partial, capped and not yet in force. To make the protection of customers against the unauthorised use of electronic payment systems real and not just nominal, India must enact legislation to replace these circulars, clearly define negligence, give customers access to evidence against them, enforce the time limit for the reversal of unauthorised transactions and share the responsibility for preventing these frauds across the entire payment chain. As digital

banking becomes the norm for even the poorest and least experienced users of banking systems, the law should recognise the safety of the payment system as a duty of the institutions that run it.

Bibliography

Cases

Roopam Kumar v. SBI Cards & Payment Services Pvt. Ltd

Barclays Bank plc v. Quincecare Ltd [1992] 4 All ER 363

Foley v. Hill (1848) 2 HL Cas 28

Jaiprakash Kulkarni v. Banking Ombudsman, 2024 SCC OnLine Bom 1666 (Bombay High Court)

Joachimson v. Swiss Bank Corporation [1921] 3 KB 110

State Bank of India v. Pallabh Bhowmick, WA No. 364/2022 (Gauhati High Court, 13 September 2024)

Tai Hing Cotton Mill Ltd v. Liu Chong Hing Bank Ltd [1986] AC 80

Statutes, rules and regulatory instruments

Banking Regulation Act 1949

Bharatiya Nyaya Sanhita 2023, ss. 318, 319

Consumer Protection Act 2019, ss. 2(7), 2(11), 2(42)

Digital Personal Data Protection Act 2023

Information Technology Act 2000, ss. 43, 43A, 46, 66C, 66D

Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011

Payment and Settlement Systems Act 2007 Reserve Bank of India Act 1934

RBI, Reserve Bank – Integrated Ombudsman Scheme 2021

RBI, Statement on Developmental and Regulatory Policies (6 February 2026)