INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 12 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

DIGITAL BANKING FRAUD IN INDIA: BANK LIABILITY AND CUSTOMER PROTECTION

AUTHOR - HARSH VARDHAN* & DR. MAYA DEVI**

* LLM STUDENT, UNIVERSITY OF LEGAL STUDIES, CHANDIGARH UNIVERSITY, MOHALI, PUNJAB, INDIA.

** ASSISTANT PROFESSOR, UNIVERSITY OF LEGAL STUDIES, CHANDIGARH UNIVERSITY, MOHALI, PUNJAB, INDIA.

BEST CITATION – HARSH VARDHAN & DR. MAYA DEVI, DIGITAL BANKING FRAUD IN INDIA: BANK LIABILITY AND CUSTOMER PROTECTION, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 6 (12) OF 2026, PG. 95-108, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

A customer who disputes an electronic transfer may be asked whether an OTP was used or a password was shared. Those questions matter, but they do not explain the whole transaction. A payment may pass the bank's authentication process even though a fraudster initiated it, while a customer may personally instruct a transfer after being deceived about its purpose. The legal consequences of these situations differ. This paper examines how Indian law distributes the resulting loss between customers, banks and payment intermediaries. It adopts a doctrinal method, reading legislation, RBI directions and judicial decisions alongside selected United Kingdom and United States materials. The analysis distinguishes the rules applicable on 14 November 2026 from the RBI amendments scheduled to apply from 1 January 2027. It finds that India already has substantial customer protection and a burden on banks to prove customer liability. The difficulty lies in classifying disputed payments and turning that burden into a reasoned examination of the evidence. The paper proposes a structured determination that identifies who initiated the transfer, examines the bank's safeguards, connects any alleged customer negligence to the loss and separates losses arising before and after notice. It also argues for accessible disclosure of transaction records and a clearer treatment of payments induced by deception. Reimbursement should follow the applicable legal category and established facts; neither the use of an OTP nor the customer's denial should decide the claim by itself.

Keywords: Digital banking; bank liability; customer negligence; electronic evidence; fraud reimbursement

I. Introduction

The legal problem in a digital banking dispute begins with a missing sum of money and two different accounts of what happened. The customer says that the payment was never intended. The bank produces a record showing a successful login and authentication. Between those positions lie questions about the person who operated the device, the instructions actually given, the warnings displayed and

the response to the first complaint. The expansion of digital payments, discussed in the RBI's Report on Currency and Finance, makes the quality of these decisions part of ordinary banking protection.[266]

The issue is wider than financial literacy. The OECD's 2026 risk monitor identifies scams and fraud as a leading concern across the jurisdictions it surveyed. Its findings provide comparative context, rather than a measure of fraud incidence in India.[267] An individual can make an avoidable mistake, but a payment service is also designed around predictable human behaviour. An assessment that looks only at the customer's final click leaves out the institution's control over authentication, monitoring and incident response.

Banking law has long examined the relationship between a payment mandate and the bank's duty of care. Ellinger's Modern Banking Law treats those questions within the wider bank–customer relationship.[268] The digital setting makes the same questions harder to investigate because the relevant records are distributed across systems that the customer cannot inspect. The resulting imbalance concerns access to proof as much as the wording of the substantive rule.

This paper asks when a bank should bear a customer's loss from digital fraud and what evidence should justify placing that loss on the customer. It uses doctrinal analysis of Indian legislation, RBI instruments and selected decisions, with a limited comparison of the United Kingdom and United States. The principal regulatory discussion concerns commercial banks within the scope of the instruments cited; rules for other categories of regulated entity require separate attention. Digital lending, data protection and cross-border enforcement are considered only where they affect the payment dispute. No interviews, survey or independent measurement of banking practices is claimed. The argument is that the existing burden of proof needs an intelligible decision process, supported by records showing how the disputed payment occurred.

The gap examined here is consequently narrower than an absence of consumer law. A bank can formally accept that it bears the burden and still reject a claim through an inference that the customer cannot meaningfully challenge. The research question is whether the decision identifies the fact proved by each record and explains the remaining inference. That inquiry also places a limit on the paper's conclusion. It can show why a proposed decision process better reflects the allocation of proof; it cannot establish how frequently banks presently follow or depart from that process without a separate empirical study.

II. Digital Banking Fraud and The Meaning of Authorisation

Authentication establishes that a system accepted specified credentials. Authorisation concerns the authority to give the payment instruction. The RBI's 2025 authentication directions define authentication through validation of customer credentials and require distinct factors, subject to stated exceptions. Compliance was generally required by 1 April 2026.[269] A transaction record may therefore

[266] Reserve Bank of India, "Digitalisation and Payment Revolution in India", *Report on Currency and Finance 2023–24* (July 29, 2024), ch. III.
[267] Organisation for Economic Co-operation and Development, *Consumer Finance Risk Monitor 2026* (OECD Publishing, Paris, 2026), section on financial scams and frauds.
[268] E.P. Ellinger, Eva Lomnicka, *et al.*, *Ellinger's Modern Banking Law* ch. 5 (Oxford University Press, Oxford, 5th edn., 2011).
[269] Reserve Bank of India, *Reserve Bank of India (Authentication Mechanisms for Digital Payment Transactions) Directions, 2025*, RBI/2025-26/79, CO.DPSS.POLC.No.S668/02-14-015/2025-2026 (September 25, 2025), paras. 3, 5 and 6.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 12 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

be strong evidence that the prescribed technical steps occurred. It does not necessarily identify the person who performed them or explain how that person obtained the credentials.

Three situations help expose the difference. A fraudster may gain access to an account and initiate a transfer without the customer's involvement. A customer may disclose credentials while believing that a caller is a bank employee, after which the caller initiates the transfer. Alternatively, the customer may personally send money to an account after being persuaded that it is a safe account or a legitimate investment. These are illustrations of different payment mechanisms. They are not findings that the same legal protection attaches to each one.

The second situation is particularly vulnerable to oversimplification. Sharing a code can be relevant to negligence without making the recipient an authorised agent for every purpose. The question is what was communicated and what followed from it. A code described as confirming a refund may in fact authorise a debit. The customer's conduct, the transaction message and the fraudster's subsequent actions must be examined together. Treating every disclosure as informed approval of the actual payment removes the very issue that the complaint asks the bank to investigate.

Research on phishing supports caution about equating successful deception with a simple lack of care. Dhamija, Tygar and Hearst's study showed how visual imitation could mislead users and how familiar browser indicators could fail to protect them. It was a small study of websites in 2006 and cannot establish the behaviour of present-day Indian banking customers.[270] Its narrower value here is explanatory: a convincing interface can cause a user to misunderstand the significance of an action. The legal assessment should examine the information available at that moment, rather than reconstruct the event with knowledge of the fraud.

There is a corresponding limit on the customer's argument. Saying that a payment was unwanted does not establish that someone else initiated it, and an ordinary contractual dispute with a merchant does not become an unauthorised banking transaction merely because the buyer regrets paying. A workable system must preserve those distinctions. Classification should precede the liability decision, so that the bank does not apply a credential-sharing rule to an entirely different type of loss.

The timing of a warning belongs in that classification. A message identifying the amount and beneficiary can help establish what the customer was asked to approve. A general warning about fraud says much less about a particular instruction. The RBI's authentication directions themselves provide for risk-based checks using features such as transaction patterns and location.[271] The evidential question should be whether the relevant message or check operated during this payment. A bank's ability to display a warning and its proof that the warning was actually delivered are not the same thing.

III. The Indian Legal and Regulatory Framework

Several legal routes can arise from the same payment. The Indian Contract Act requires performance of contractual promises and permits compensation for loss caused by breach, subject to its rules on recoverable damage.[272] Those provisions help frame a claim concerning an unfulfilled

[270] Rachna Dhamija, J.D. Tygar and Marti Hearst, "Why Phishing Works", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* 581–590 (2006), at 581–582.
[271] RBI, *Authentication Directions*, *supra* note 4, para. 8.
[272] The Indian Contract Act, 1872 (Act 9 of 1872), ss. 37 and 73.

banking obligation, but they do not themselves supply the detailed allocation rules for every electronic fraud. The contractual mandate must be read alongside the regulatory duties governing the institution and the disputed service.

The RBI's role rests on statutory powers, including its power to issue directions under section 35A of the Banking Regulation Act.[273] The Payment and Settlement Systems Act separately provides the framework for regulating payment systems and gives the RBI power to issue directions.[274] This matters because a digital payment is commonly performed through several participants. The powers and obligations applicable to an account-holding bank cannot simply be assumed to be identical to those of every technology company involved in the transaction.

The Information Technology Act addresses unauthorised computer-related acts and offences such as identity theft and cheating by personation through a computer resource.[275] Cheating and cheating by personation are also addressed in the Bharatiya Nyaya Sanhita.[276] These provisions are relevant to the fraudster's conduct. Establishing a criminal offence, however, does not by itself answer whether the bank breached a payment obligation or whether the customer qualifies for reimbursement. The recovery claim and the prosecution may concern the same events while asking different legal questions.

The Consumer Protection Act supplies another route where the complainant satisfies the statutory requirements. Its definition of service includes banking, while deficiency concerns shortcomings in the quality or manner of performance required by law or undertaken by the provider. The available orders include compensation for loss or injury attributable to the opposite party's negligence.[277] A consumer claim still requires attention to the relevant service failure and evidence. The occurrence of fraud is not a complete explanation of the bank's liability.

The RBI's July 2017 circular established a more specific scheme for unauthorised electronic banking transactions, distinguishing bank fault, customer negligence and third-party breaches. It also placed the burden of proving customer liability on the bank.[278] For the commercial banks covered here, the consolidated Responsible Business Conduct Directions, 2025 now provide the relevant regulatory text. Bank negligence attracts zero customer liability. In qualifying third-party breaches, notification within three working days of the bank's communication attracts zero liability; later reporting is treated differently. Proven customer negligence can make the customer bear the loss until reporting, while subsequent unauthorised loss falls on the bank.[279] The familiar three-day protection therefore cannot be treated as an unconditional rule for every fraudulent payment.

The final component is evidence. Sections 61 to 63 of the Bharatiya Sakshya Adhiniyam govern the treatment of electronic records, including the conditions for specified computer outputs.[280] They

273 The Banking Regulation Act, 1949 (Act 10 of 1949), s. 35A.
274 The Payment and Settlement Systems Act, 2007 (Act 51 of 2007), ss. 2(1)(c) and 18.
275 The Information Technology Act, 2000 (Act 21 of 2000), ss. 43, 66C and 66D.
276 The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), ss. 318 and 319.
277 The Consumer Protection Act, 2019 (Act 35 of 2019), ss. 2(11), 2(42) and 39(1)(d).
278 Reserve Bank of India, "Customer Protection—Limiting Liability of Customers in Unauthorised Electronic Banking Transactions", RBI/2017-18/15, DBR.No.Leg.BC.78/09.07.005/2017-18 (July 6, 2017), paras. 6–12.
279 Reserve Bank of India, *Reserve Bank of India (Commercial Banks—Responsible Business Conduct) Directions, 2025*, RBI/2025-26/170, DOR.MCS.REC.No.89/01-01-032/2025-26 (November 28, 2025; updated October 1, 2026), paras. 67–71.
280 The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), ss. 61–63.

concern proof in proceedings to which the enactment applies; they should not be converted into a claim that a customer must obtain a forensic certificate before the bank will register a complaint. The bank's internal investigation, the ombudsman process and court proceedings perform different functions. Confusing their requirements can deny a customer an effective first response.

These routes should also be kept distinct in the pleading. A complaint seeking restoration of an unauthorised debit may raise the bank's authority to debit the account, whereas a compensation claim for consequential loss requires its own basis and proof. Section 73 of the Contract Act does not permit every asserted consequence to be recovered simply because a breach occurred.[281] The article's proposed classification is intended to clarify the primary payment loss. It leaves additional damages to the applicable rules on causation, remoteness and proof, rather than treating the reimbursement amount as a complete measure of every possible claim.

IV. Allocation of Liability Among Banks and Payment Intermediaries

The account-holding bank is usually the institution from which the customer seeks restoration of the debit. Yet the mobile interface, payment gateway, communications network and recipient account may involve other organisations. The important distinction is between the customer's entitlement against a particular institution and the allocation of responsibility among the participating firms. A bank may have a contractual claim against a service provider without being entitled to suspend a customer's established reimbursement claim until that separate dispute is resolved.

The RBI's outsourcing directions expressly preserve the bank's obligations and ultimate responsibility for outsourced activity. They also protect customers' rights to seek redress against the bank.[282] This principle prevents the use of outsourcing as a routine answer to a service complaint. Its reach nevertheless depends on the relationship involved. An independent application or telecommunications service is not automatically the bank's outsourced agent. The investigation should identify that relationship, the function performed and the governing regulatory duties before assigning responsibility.

The Financial Stability Board's third-party risk toolkit offers a useful institutional perspective. It treats dependency on external providers as a risk that financial institutions must identify and manage across the service relationship. The toolkit is guidance, not an Indian compensation rule.[283] Its relevance is that external provision does not make a risk disappear from the institution's governance. In a customer dispute, the practical implication is to ask which party retained the records and which party was expected to respond when the system identified danger.

The Digital Payment Security Controls Directions, 2026 require monitoring for suspicious behaviour and identify relevant indicators, including transaction velocity, unusual locations and new beneficiaries.[284] Such requirements give substance to an inquiry into bank conduct. A bank may establish that an unusual payment was reviewed and reasonably allowed. It may instead reveal that

[281] The Indian Contract Act, 1872 (Act 9 of 1872), s. 73.
[282] Reserve Bank of India, *Reserve Bank of India (Commercial Banks—Managing Risks in Outsourcing) Directions, 2025*, RBI/DOR/2025-26/171, DOR.ORG.REC.No.90/21-04-158/2025-26 (November 28, 2025), paras. 9, 17, 49 and 93–94.
[283] Financial Stability Board, "Enhancing Third-Party Risk Management and Oversight: A Toolkit for Financial Institutions and Financial Authorities", Final Report (December 4, 2023), sections on the lifecycle of third-party relationships.
[284] Reserve Bank of India, *Reserve Bank of India (Commercial Banks—Digital Payment Security Controls) Directions, 2026*, RBI/DoS/2026-27/411, DoS.CO.CSITEG.5/31.01.015/2026-27 (July 31, 2026; updated October 1, 2026), paras. 52–57.

an alert was generated but ignored. Neither conclusion follows from the mere fact that the payment succeeded. The appropriate inquiry concerns the control required for that transaction and what the institution actually did.

There are costs on both sides. An indiscriminate blocking policy can prevent legitimate transfers and inconvenience customers. A policy of allowing any correctly authenticated transaction can leave obvious warning signs unused. The suggested liability test should therefore examine a concrete missed precaution, its practicability and its probable effect. It should not treat a successful fraud as conclusive proof that the bank's entire security system was defective. Equally, the bank should not be allowed to answer a specific allegation about an ignored alert with a general statement that its platform follows industry standards.

Allocation between firms requires the same precision. If a recipient bank receives an actionable request to preserve funds, the response may affect the amount ultimately recoverable. That possible responsibility is distinct from the sending bank's original authority to debit its customer. The proposed approach would record each institution's role without making the customer prove the entire interbank chain before receiving relief to which the governing rules already entitle them. Later recovery should be reconciled against sums already restored. This preserves recourse between institutions while avoiding a process in which each participant simply refers the customer to another.

V. Customer Negligence and The Burden of Proof

Negligence must describe conduct that can be examined. "The customer was careless" supplies no account of the event. A reasoned decision should identify the act alleged, the information available to the customer and the connection between that act and the disputed debit. Sharing a password after a clear warning differs from entering details into a convincing imitation of the bank's own page. The distinction does not automatically excuse the second customer. It identifies the circumstances that need to be proved before responsibility is assigned.

Sasse, Brostoff and Weirich argue that blaming users without examining the causes of their behaviour will not produce effective security. Their analysis considers memory, task demands and the support available to users.[285] Applied to the present problem, that is a reason to assess whether precautions are usable. A lengthy notice displayed during account opening may have less value in preventing a particular fraud than a clear warning delivered when a new payee is added. This is a proposed way of assessing precautions, rather than a statement that every ineffective warning creates legal liability.

The burden of proving customer liability already lies on the bank under the current commercial-bank directions.[286] The reform needed is consequently more precise than a demand to reverse the burden. The bank should explain how the records discharge it. Evidence that an OTP was generated, evidence that it was delivered and evidence that the customer entered it are different propositions. Even proof of entry may leave a further question about the person who entered it and the

[285] M. Angela Sasse, Sacha Brostoff and Dirk Weirich, "Transforming the 'Weakest Link'—A Human/Computer Interaction Approach to Usable and Effective Security", 19(3) *BT Technology Journal* 122–131 (2001), at 122–125.
[286] RBI, *Responsible Business Conduct Directions*, *supra* note 14, para. 75.

circumstances under which the code was obtained. A conclusion should address those steps where they are genuinely disputed.

Anderson's early examination of payment security documented failures arising from implementation and management, rather than from defeating cryptographic theory alone.[287] The study is not evidence that a particular contemporary Indian transaction suffered such a failure. It supports a narrower methodological point: the reliability of one component should not be used as proof that the entire transaction could only have occurred through customer fault. An investigator needs a transaction-specific account that remains open to competing explanations.

Electronic evidence also has to be distinguished from its interpretation. In *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, the Supreme Court explained the certificate requirement under the earlier evidence legislation and the means of seeking a certificate from the person controlling the record.[288] The decision remains relevant to the problem of a party lacking possession of the system, while current proceedings require attention to the applicable evidence enactment. A properly produced record can show that the system recorded an event. Whether the event proves informed approval, disclosure of a credential or negligent conduct remains a matter of inference.

A customer should provide a prompt account, preserve available messages and cooperate with reasonable inquiries. These responsibilities do not require the customer to identify the precise malware or prove an internal banking defect before the bank examines its own logs. A sensible disclosure process would provide a readable chronology, explain material records and allow correction of mistaken assumptions. Security-sensitive details could be restricted or redacted, but that concern should be addressed specifically. A refusal letter that says only "authenticated using OTP" gives the customer little opportunity to challenge an error and gives a later reviewer little basis for assessing the decision.

There is a further distinction between admitting a record and accepting everything said about it. The electronic-record provisions concern the legal treatment of the output.[289] A certified log showing access from an IP address may still require explanation before it identifies a particular person. A record of an alert may establish its generation without establishing receipt. The customer must be able to contest those inferences without having to deny the existence of the record itself. This distinction would also help banks: a properly explained chronology may resolve an apparently suspicious event more convincingly than a large, unexplained bundle of technical material.

VI. Judicial Approaches and Customer Remedies

The older law on payment mandates remains useful, provided its factual setting is respected. In *Canara Bank v. Canara Sales Corporation*, the Supreme Court rejected the bank's attempt to debit the customer for forged cheques in the circumstances before it. The decision examined mandate, knowledge and the proposed defence based on the customer's failure to discover the fraud.[290] Its relevance to electronic banking lies in the need to establish authority for a debit. It cannot simply

287 Ross Anderson, "Why Cryptosystems Fail", *Proceedings of the First ACM Conference on Computer and Communications Security* 215–227 (1993), at 215–217.
288 (2020) 7 SCC 1, paras. 41–45.
289 The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023), ss. 62–63.
290 (1987) 2 SCC 666.

displace later RBI rules that expressly attach consequences to customer negligence and reporting delays. A forged signature and a transfer personally instructed after deception raise different problems of authority.

State Bank of India v. Pallabh Bhowmick provides a more direct electronic banking example. In its reasoned order dismissing the bank's special leave petition, the Supreme Court agreed with findings that the transactions were unauthorised and fraudulent and that customer negligence had not been established. It also noted the customer's notification within 24 hours. The Court's caution that customers could be negligent in other circumstances is part of the order's significance.[291] The decision supports protection where the relevant findings favour the customer; it does not make banks insurers of every disputed payment.

The later Delhi High Court decision in *State Bank of India v. Hare Ram Singh* exposes the other side of the problem. The Division Bench allowed the bank's appeal against an order directing full reimbursement. It treated customer negligence as potentially extending beyond express disclosure of an OTP and held that the disputed technical issues could not be conclusively decided through the assumptions made in writ proceedings. The Court referred to the need for technical and forensic examination on evidence.[292] It would therefore be inaccurate to present this case as another straightforward award in favour of a fraud victim.

Read together, these decisions caution against presumptions favouring either side. They also expose a practical problem for the customer. If technical proof is necessary, the institution controlling that proof must explain its records in a form that can be tested. Otherwise, a formally correct insistence on evidence may leave the claimant with no affordable means of obtaining it. That concern does not justify assuming a banking failure. It supports a procedural requirement that a bank which alleges customer responsibility produce a coherent explanation of the material available to it.

Redress begins before litigation. Under the present directions, the bank must provide the prescribed shadow reversal within ten working days of notification, with value dating, and resolve the complaint within the applicable period, which cannot exceed 90 days.[293] Provisional credit and final liability should be kept distinct. A provisional measure protects the position pending investigation; it does not remove the obligation to reach a properly reasoned final decision.

The Integrated Ombudsman Scheme, 2026 provides an external route for eligible service complaints and has applied from 1 July 2026, subject to its transitional arrangements. Its maintainability requirements include first approaching the regulated entity and restrictions concerning the same grievance before other adjudicatory forums.[294] These conditions matter when choosing a remedy. The paper does not treat an ombudsman complaint, a consumer proceeding and a writ petition as freely interchangeable steps that can all be pursued simultaneously for the same grievance.

A qualifying consumer may seek compensation under the Consumer Protection Act, but the pleading should identify the service failure and resulting loss.[295] A complaint might concern an

291 SLP (C) No. 30677 of 2024, Supreme Court of India, order dated January 3, 2025, paras. 1–7.
292 2026:DHC:4833-DB, LPA No. 52 of 2025, Delhi High Court, judgment dated May 29, 2026, paras. 9.1–9.7 and 15–19.
293 RBI, *Responsible Business Conduct Directions*, *supra* note 14, paras. 72–73.
294 Reserve Bank of India, *Reserve Bank—Integrated Ombudsman Scheme, 2026* (effective July 1, 2026), cls. 1 and 10.
295 The Consumer Protection Act, 2019 (Act 35 of 2019), s. 39(1)(d).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 12 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

unauthorised debit, a failure to act after notice, or an unexplained rejection of a reimbursement claim. Each requires its own factual account. Recovery from the fraudster, regulatory reimbursement and compensation for a separate proven service failure should also be accounted for, so that the customer is restored without receiving double recovery for the same loss.

Cost is especially relevant when the disputed amount is too small to justify extensive forensic litigation. Requiring technical scrutiny, as the Delhi High Court's discussion indicates, does not itself provide a means of obtaining that scrutiny.[296] A fair process should allow a focused request for the records that decide the disputed point. It should not routinely demand a complete examination of every device and system involved. This is a procedural proposal arising from the difficulty identified in the cases, rather than a claim that the courts have already prescribed a single investigative method for all banking complaints.

VII. Comparative Lessons from The United Kingdom and United States

The United Kingdom separates consent to a payment from evidence that the payment system authenticated it. The Payment Services Regulations address consent, proof of authentication and the consequences of an unauthorised transaction. Regulation 75 makes clear that recorded use of a payment instrument is not necessarily sufficient, by itself, to prove authorisation or the relevant customer misconduct.[297] The lesson for India is evidential. A transaction can be technically valid within the system while the legal significance of the customer's conduct remains disputed.

Philipp v. Barclays Bank UK PLC demonstrates the limit of relying on ordinary mandate principles to protect a person who personally instructs a fraudulent payment. The UK Supreme Court declined to extend the asserted Quincecare duty to the clear instructions personally given by the customer in that case. Its analysis distinguished those instructions from an agent's dishonest misuse of authority.[298] The result shows why unauthorised transfers and authorised push payment scams need separate treatment. It does not establish that payment providers can never have duties under regulation, contract or a reimbursement scheme concerning scams.

The Payment Systems Regulator subsequently implemented a reimbursement framework for qualifying Faster Payments authorised push payment scams, beginning on 7 October 2024. The final policy addresses a consumer standard of caution and exceptions rather than making reimbursement unconditional.[299] A separate policy statement fixed the maximum reimbursement at £85,000 per claim.[300] These materials concern a defined payment-system regime. They should not be cited as proof that every British fraud victim, including one using an overseas payment route, receives automatic reimbursement.

The United States supplies a different comparison. The Electronic Fund Transfer Act places the burden on the financial institution to establish authorisation or the conditions for imposing liability in a

296 2026:DHC:4833-DB, LPA No. 52 of 2025, Delhi High Court, judgment dated May 29, 2026, paras. 15–16.
297 The Payment Services Regulations 2017 (United Kingdom), S.I. 2017/752, regs. 67 and 75–77.
298 [2023] UKSC 25, paras. 97–100.
299 Payment Systems Regulator, "Fighting Authorised Push Payment Scams: Final Decision", Policy Statement PS23/4 (2023), sections on the consumer standard of caution and implementation.
300 Payment Systems Regulator, "Faster Payments APP Scams Reimbursement Requirement: Confirming the Maximum Level of Reimbursement", Policy Statement PS24/7 (2024).

dispute within section 1693g.[301] Regulation E further provides that consumer negligence cannot enlarge liability beyond its permitted limits. Its definition of an unauthorised electronic fund transfer and its error-resolution provisions remain essential to the protection's scope.[302] These rules should not be taken to erase the distinction between a fraudster initiating a payment with stolen credentials and a customer personally initiating a payment after deception.

The useful comparison is therefore selective. India can examine the UK treatment of recorded authentication and the US constraint on expanding customer liability through general negligence arguments. A reimbursement regime for customer-initiated scams requires its own coverage rules, incentives and funding choices. Direct transplantation would overlook differences in payment systems and institutional capacity. The comparative materials are strongest when used to test a particular Indian rule: what the bank must prove, what conduct matters and which losses remain outside the specified protection.

For example, excluding ordinary negligence from additional liability, as Regulation E does within its scope, is a substantive policy choice rather than merely a rule about evidence.[303] It could encourage institutions to invest in prevention, but a proposal for India would still need to consider reporting duties, fraudulent claims and the distribution of costs. Those effects cannot be settled by citation to the foreign rule alone. The present proposal accordingly concentrates on a change that can operate within India's existing allocation: requiring the institution to make its reasons and material evidence intelligible.

VIII. Regulatory Reform and A Proposed Liability Test

The June 2026 amendment to the commercial-bank conduct directions is an important development, but it applies to transactions undertaken on or after 1 January 2027. It introduces a broader fraudulent-transaction framework, keeps the burden of proving customer liability on the bank and changes relevant reporting and disposal periods. It also creates a conditional small-value compensation mechanism for specified customer-negligence cases.[304] These changes must be evaluated as enacted future requirements, rather than treated as either a consultation draft or a remedy already available for every earlier loss.

Two choices deserve scrutiny. The third-party-breach rule changes the reporting measure from receipt of the bank's communication to five calendar days from occurrence. That can be significant where the customer learns of the transaction late. The small-value mechanism covers qualifying gross losses up to Rs. 50,000, with compensation of 85 per cent of net loss or Rs. 25,000, whichever is lower, and includes a once-in-a-lifetime condition and a stated one-year period of operation.[305] The mechanism offers relief, but its limits leave a policy question about repeated victimisation and losses just beyond the eligibility threshold.

---

301 The Electronic Fund Transfer Act, 1978 (United States), 15 U.S.C. § 1693g(b).

302 Consumer Financial Protection Bureau, *Regulation E*, 12 C.F.R. Part 1005, with official interpretations, ss. 1005.2(m), 1005.6 and 1005.11; official interpretation 6(b)-2.

303 *Id.*, official interpretation 6(b)-2.

304 Reserve Bank of India, *Reserve Bank of India (Commercial Banks—Responsible Business Conduct) Third Amendment Directions, 2026*, RBI/2026-27/167, DOR.MCS.REC.No.130/01-01-032/2026-27 (June 24, 2026), paras. 3(2) and 4; substituted paras. 76K–76U.

305 *Id.*, substituted paras. 76M, 76T and 76U.

The definition of fraudulent transactions also requires careful application. It expressly includes third-party use of fraudulently obtained credentials and customer approval under coercion or duress.[306] It should not be assumed that every payment personally initiated after a false representation necessarily falls within those words. A future clarification could distinguish deception about the recipient or purpose from coercion affecting the instruction. Without that distinction, disputes may move from the meaning of "unauthorised" to an equally uncertain argument about what kind of deception the new category covers.

The paper proposes a structured liability determination within the applicable regulatory framework. The first finding should identify who initiated the payment and the authority claimed for doing so. The second should identify any relevant failure of a bank or intermediary, including what happened to a material security alert. The third should state the precise customer conduct alleged and explain how it contributed to the particular loss. Reporting and the consequences of any delay should then be assessed under the rule applicable to the transaction date. This would make the existing allocation rules easier to apply; it would not authorise an investigator to invent a different liability cap.

The proposal also requires a distinction between causing a fraud and failing to prevent an additional loss. Consider a customer who discloses a credential but promptly reports the first debit. If further debits occur because the bank fails to restrict the account after receiving notice, those later transactions require a separate explanation. Conversely, if the bank acted promptly and the entire loss had already occurred, a general criticism of its complaint handling does not prove that it caused the original debit. Keeping the chronology visible permits responsibility to follow the loss actually connected to the alleged failure.

For this process to work, the rejection decision should disclose an accessible sequence of events and the records materially relied upon. It should distinguish facts established by logs from inferences about the customer's actions. Where a serious technical dispute remains, an independent reviewer should be able to request the relevant records, with proportionate protection for security-sensitive information. An adverse inference from missing material should depend on control of the record, a reasonable preservation obligation and the explanation for its absence. It should not arise merely because a transaction is difficult to reconstruct.

Where neither customer negligence nor a bank failure has been established, the investigator should return to the relevant third-party-breach rule and the proved reporting time. An unresolved case should not be silently recategorised as customer negligence. Equally, the proposed test should not erase the conditions attached to third-party protection or substitute an unrestricted fairness discretion. Recording an express finding that a necessary fact remains unproved would make the operation of the burden visible. It would show whether the final result follows from established misconduct, a reporting rule or a failure by the institution to prove the liability it alleges.

These procedural measures would require evaluation in practice. Published, anonymised decisions could reveal whether similar disputes are classified consistently, while reporting could distinguish proven customer negligence from claims rejected for lack of information. The OECD's discussion of

[306] *Id.*, para. 4(3), inserting para. 4(15A).

measuring consumer-protection outcomes supports attention to what remedies deliver, rather than relying only on their formal existence.[307] The immediate research finding remains limited: Indian law contains substantial protection, but a usable explanation of the evidence is necessary if that protection is to guide the decision in an individual dispute.

IX. Conclusion

Digital banking fraud does not produce a single question of liability. A stolen-credential transfer, a payment enabled by negligent disclosure and a payment personally instructed after deception may call for different legal treatment. Indian law already recognises bank duties, customer responsibilities and a burden of proof on banks. The task is to apply those rules to an established account of what occurred.

The cases examined do not support an unconditional right to reimbursement or a presumption that successful authentication proves customer fault. They require attention to findings, procedural setting and the applicable regulatory category. The proposed approach makes that attention systematic: identify the instruction, examine the safeguards, connect alleged negligence to the loss and account separately for events after notice. Its value would lie in decisions that the customer and an external reviewer can understand and test.

The forthcoming 2027 framework creates an opportunity to improve this process, while leaving questions about reporting periods, limited compensation and customer-initiated scams. Clear treatment of those questions should accompany meaningful access to evidence. A bank's conclusion deserves acceptance when it explains the transaction and satisfies the applicable rule; its institutional possession of the records should not substitute for that explanation.

References

Indian legislation

The Indian Contract Act, 1872 (Act 9 of 1872).

The Banking Regulation Act, 1949 (Act 10 of 1949).

The Information Technology Act, 2000 (Act 21 of 2000).

The Payment and Settlement Systems Act, 2007 (Act 51 of 2007).

The Consumer Protection Act, 2019 (Act 35 of 2019).

The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023).

The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).

RBI directions and official report

Reserve Bank of India, "Customer Protection—Limiting Liability of Customers in Unauthorised Electronic Banking Transactions", RBI/2017-18/15, DBR.No.Leg.BC.78/09.07.005/2017-18 (July 6, 2017).

[307] OECD, *Consumer Finance Risk Monitor*, *supra* note 2, section on defining objectives and measuring effectiveness.

Reserve Bank of India, *Reserve Bank of India (Commercial Banks—Responsible Business Conduct) Directions, 2025*, RBI/2025-26/170, DOR.MCS.REC.No.89/01-01-032/2025-26 (November 28, 2025; updated October 1, 2026).

10. Reserve Bank of India, *Reserve Bank of India (Commercial Banks—Responsible Business Conduct) Third Amendment Directions, 2026*, RBI/2026-27/167, DOR.MCS.REC.No.130/01-01-032/2026-27 (June 24, 2026).

11. Reserve Bank of India, *Reserve Bank of India (Commercial Banks—Digital Payment Security Controls) Directions, 2026*, RBI/DoS/2026-27/411, DoS.CO.CSITEG.5/31.01.015/2026-27 (July 31, 2026; updated October 1, 2026).

12. Reserve Bank of India, *Reserve Bank of India (Authentication Mechanisms for Digital Payment Transactions) Directions, 2025*, RBI/2025-26/79, CO.DPSS.POLC.No.S668/02-14-015/2025-2026 (September 25, 2025).

13. Reserve Bank of India, *Reserve Bank of India (Commercial Banks—Managing Risks in Outsourcing) Directions, 2025*, RBI/DOR/2025-26/171, DOR.ORG.REC.No.90/21-04-158/2025-26 (November 28, 2025).

14. Reserve Bank of India, *Reserve Bank—Integrated Ombudsman Scheme, 2026* (effective July 1, 2026).

15. Reserve Bank of India, "Digitalisation and Payment Revolution in India", *Report on Currency and Finance 2023–24* (July 29, 2024).

Indian judicial decisions

16. *Canara Bank v. Canara Sales Corporation* (1987) 2 SCC 666.

17. *State Bank of India v. Pallabh Bhowmick*, SLP (C) No. 30677 of 2024, Supreme Court of India, order dated January 3, 2025.

18. *State Bank of India v. Hare Ram Singh*, 2026:DHC:4833-DB, LPA No. 52 of 2025, Delhi High Court, May 29, 2026.

19. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* (2020) 7 SCC 1.

Comparative legislation decisions and regulatory materials

20. The Payment Services Regulations 2017 (United Kingdom), S.I. 2017/752.

21. *Philipp v. Barclays Bank UK PLC* [2023] UKSC 25.

22. Payment Systems Regulator, "Fighting Authorised Push Payment Scams: Final Decision", Policy Statement PS23/4 (2023).

23. Payment Systems Regulator, "Faster Payments APP Scams Reimbursement Requirement: Confirming the Maximum Level of Reimbursement", Policy Statement PS24/7 (2024).

24. The Electronic Fund Transfer Act, 1978 (United States), 15 U.S.C. § 1693 et seq.

25. Consumer Financial Protection Bureau, *Regulation E*, 12 C.F.R. Part 1005, with official interpretations.

Academic literature and policy reports

26. Ross Anderson, "Why Cryptosystems Fail", *Proceedings of the First ACM Conference on Computer and Communications Security* 215–227 (1993). DOI: 10.1145/168588.168615.

27. M. Angela Sasse, Sacha Brostoff and Dirk Weirich, "Transforming the 'Weakest Link'—A Human/Computer Interaction Approach to Usable and Effective Security", 19(3) *BT Technology Journal* 122–131 (2001). DOI: 10.1023/A:1011902718709.

28. Rachna Dhamija, J.D. Tygar and Marti Hearst, "Why Phishing Works", *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* 581–590 (2006). DOI: 10.1145/1124772.1124861.

29. Organisation for Economic Co-operation and Development, *Consumer Finance Risk Monitor 2026* (OECD Publishing, Paris, 2026). Available at: https://doi.org/10.1787/61f7dbe0-en (last visited on November 14, 2026).

30. Financial Stability Board, "Enhancing Third-Party Risk Management and Oversight: A Toolkit for Financial Institutions and Financial Authorities", Final Report (December 4, 2023).

31. E.P. Ellinger, Eva Lomnicka, *et al.*, *Ellinger's Modern Banking Law* (Oxford University Press, Oxford, 5th edn., 2011).