INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

ISSN: 2582-6433

November 2026

RESEARCH ARTICLE

Liability in E-Cheque Transactions: Determining the Responsibility of Banks, Account Holders and Certifying Authorities

S. Padmasri

SASTRA Deemed University

www.ijlra.com

ABOUT THE JOURNAL

International Journal for Legal Research and Analysis (IJLRA)

ISSN: 2582-6433

IJLRA provides a platform for scholarly writing and discussion on law, legal research and interdisciplinary questions. Research articles explore legal principles, institutions, policy and contemporary developments.

Journal website: www.ijlra.com

PUBLICATION INFORMATION

International Journal for Legal Research and Analysis

ISSN: 2582-6433

Editorial note

The views and arguments expressed in this article are those of its author(s). Readers should consult the original legal authorities and sources cited in the manuscript.

Copyright and permissions are subject to the applicable publication agreement.

ARTICLE DETAILS

Liability in E-Cheque Transactions: Determining the Responsibility of Banks, Account Holders and Certifying Authorities

Author: S. Padmasri

Institution: SASTRA Deemed University

Journal: International Journal for Legal Research and Analysis

ISSN: 2582-6433

Liability in E-Cheque Transactions: Determining the Responsibility of Banks, Account Holders and Certifying Authorities

S. Padmasri

SASTRA Deemed University

ABSTRACT

The emergence of electronic cheques as a digital substitute for paper cheques has transformed the banking sector by facilitating secure, paperless, and efficient financial transactions. E-cheques rely on digital signatures, electronic authentication, and Public Key Infrastructure, thereby involving multiple stakeholders, including account holders, banks, and Certifying

Authorities. However, the increasing incidence of cyber frauds such as identity theft, digital signature compromise, unauthorized issuance of e-cheques, phishing attacks, and electronic manipulation of payment instructions has raised complex legal questions concerning liability and accountability.

The existing framework governing e-cheque transactions in India is primarily derived from IT Act,

2000, NI Act, 1881, RBI regulations, and provisions relating to electronic records and digital signatures. The paper examines the legal framework, judicial precedents and regulatory mechanisms governing e-cheque frauds, with particular emphasis on determining responsibility for financial loss. The study seeks to identify legal gaps, analyze evidentiary and jurisdictional challenges, and propose reforms for establishing a coherent liability regime capable of ensuring consumer protection and cyber security in electronic banking transactions.

Key Words: E-Cheques; Cyber Fraud; Bank Liability; Certifying Authorities; Holder in Due

Course.

INTRODUCTION

Background of the Study

Cheques remain a usual method of making commercial payments in India and are ruled by the

Negotiable Instruments Act, 1881. The 2002 amendment brought cheques into the digital framework by recognising electronic cheques and electronic images of truncated cheques under

Section 6 of Information Technology Act. 1 An electronic cheque is created digitally and authenticated using a digital or electronic signature.2

The private key is held with the subscriber. the public key is linked to subscriber by certificate given by Certifying Authority (CA). The drawee bank then uses this certificate to verify the digital signature.2 Each actor controls one link: the account holder - the private key, the CA - the certificate, and the bank - verification and payment. When a fraud succeeds, the loss must land on one of them, and the statute book does not say which.

Phishing, vishing, stolen login details, and harmful mobile applications related frauds are frequently faced by the banks,3 and Courts have already dealt with SIM-swap frauds where the authentication went through even though the customer had not approved the payment. This creates the base problem.5 With a paper cheque, a forged signature means there was no authority to bank, to debit from account of the customer.4 In electronic world, a signature created with a stolen private key verifies perfectly. Mathematics confirms integrity, not authority.

In addition to the factors discussed earlier, the current study is relevant for another reason, negotiability. The value of a negotiable instrument comes from the protection given to a holder

1 Negotiable Instruments Act 1881; s 6, NI (Amendment and Miscellaneous Provisions) Act 2002; Vijayashankar Na, 'Cheque in Electronic Form, Redefined, Implications on E- Banking' 2NI Act 1881 (n 1) s 6, Explanation I(a).

2 Information Technology Act 2000, ss 21, 35–42.

3 ELP, 'RBI Tightens Customer Protection Framework for Fraudulent Electronic Banking Transactions'

5Subodh C Korde v Union of India 2026 SCC OnLine Bom 3629, as reported in ELP (n 4).

4 Canara bank v canara sales corporation case (1987) 2 SCC 666.

in due course, who can receive it without being affected by defects in the previous holder's title.5 Commentators have pointed out that the NI Act was not later amended to clearly explain how endorsement or the concept of a holder in due course would apply to electronic cheques.

As a result, some provisions still have to be understood by applying the existing rules by analogy. 6 Comparative commentators have pointed out that negotiable instruments law is becoming outdated and does not always fit modern digital transactions, 7 the UNCITRAL

Model Law on Electronic Transferable Records (MLETR) addresses this issue by treating electronic records as functionally equivalent to paper documents and using the idea of 'control' instead of physical possession.8 Whether an Indian payee who receives an e-cheque ever be a

HDC, and against whom that status is good, is the central added issue examined here.

The RBI has also brought in the Third Amendment Directions, 2026 to update the rules that protect customers from fraudulent electronic banking transactions. The revised rules will apply to transactions made on or after 1 January 2027.9

LITERATURE REVIEW

Negi's paper, published on SSRN, looks at how e-cheques work in India. It notes that cheque truncation was first tested in the National Capital Region in February 2008, and that the NI Act and IT Act were amended to support this system.10 Gopala Krishna and Vidya, writing in a banking trade publication, explain the changes made to Section 6 and point out that banks could

5 NI Act 1881 (n 1) ss 9, 36, 53.

6 Na (n 1).

7 'In Search for the Optimal Law Governing Digital Payment Rights' (Oxford Business Law Blog, 2 February 2026)

8 Henry D Gabriel, 'The UNCITRAL Model Law on Electronic Transferable Records' (2019) 24(2) Uniform Law Review 261, 261 (legal recognition and functional equivalence). On 'control' (MLETR art 11) see 'The Right of Control over Electronic Negotiable Documents and Electronically Documented Rights and Goods' (Springer Nature Link).

9 ELP (n 4).

10 Chitranjali Negi, 'E-Cheque Structure in India' (SSRN, 16 July 2015) face legal risks if they use an authentication method other than the one provided under Section

3(2) of the IT Act.11 Both sources mainly explain the existing framework and were written before the current regulatory position.

Steennot, in Computer Law & Security Report, compares the European Payment Services

Directive with the United States Electronic Funds Transfer Act (EFTA). He observes the transactions made through cheque or similar paper instruments were excluded by EFTA, argues that the European regime creates important risks for the holder of an electronic payment instrument, and identifies the role of gross negligence as the weakness of the European approach.12 Donnelly reviews the PSD II regime and concentrates on the allocation of liability in case of unauthorized transactions as well as the new security and authentication obligations introduced, and the loopholes existing within the current scheme.13 Both show that allocation by fault and authentication standard is the dominant comparative technique; neither addresses negotiable instruments.

Gabriel explains that the MLETR gives statutory acknowledgement to electronic transferable evidence and treats them on same way as paper records.14 His work guides how holder-in-due-course protection might be rebuilt without paper possession.

Jain's recent doctrinal study reveals that the Indian RBI's 2017 circular creates a normative disconnect: while the regime shifts the evidentiary burden to the banks, the courts that hear such disputes are either unprepared to evaluate this burden or unwilling to assert jurisdiction once fraud is alleged. He refers to the different rulings of the Single Judge and Division Bench

11 V Gopala Krishna and C Vidya, 'Electronic Cheques and Evidentiary Value' (2005) Professional Banker (April)

12 Reinhard Steennot, 'Allocation of Liability in Case of Fraudulent Use of an Electronic Payment Instrument: The New Directive on Payment Services in the Internal Market' (2008) 13 Mary Donnelly, 'Payments in the Digital Market: Evaluating the Contribution of Payment Services Directive II' (2016)

14 Gabriel (n 10) 261.

in the Hare Ram Singh proposed that banks should be presumed liable unless they can show otherwise. He also suggests the use of technical assessors and forensic audit trails.15

RESEARCH PROBLEM

The Negotiable Instruments Act 1881, the Information Technology Act 2000 (IT Act) and

RBI's customer-protection directions each touch e-cheque fraud, but none clearly states how loss is to be shared among the drawer, the drawee bank, the CA and a payee claiming as

HDC. NI Act regulates the instrument but, drafted around paper; the IT Act regulates keys and certificates but speaks of liability only sparingly; and the RBI directions allocate burden of proof for electronic banking transactions without expressly naming e-cheques. The problem is whether the existing Indian framework yields an adequate and coherent liability regime for fraudulent e-cheque transactions, with particular attention to the position of the holder in due course.

RESEARCH OBJECTIVES

1. To map the statutory, regulatory and common-law sources that allocate loss in fraudulent e-cheque transactions.

2. To examine whether the forged-cheque rule of Canara Bank is justified where the signature of the drawer has been digitally signed and found to be genuine.

15 Kairavi Jain, 'Beyond Zero Liability: Re-Examining Customer Protection and Bank Accountability for Cyber Fraud under the RBI's 2017 Framework and Its 2026 Reforms' (2026)

3. To determine whether a payee can qualify as a holder in due course of an e-cheque under section 9 of the NI Act and what reliance on a CA's certificate is required.

4. To examine the exposure of CAs to relying parties and the extent to which RBI directions bind or displace statutory duties.

5. To suggest ways to improve the liability framework.

RESEARCH QUESTIONS

1. Does section 42 of the IT Act, which keeps a subscriber liable until compromise of a private key is reported, displace the rule that a forged cheque confers no mandate on the bank, and if so to what extent?

2. Can a payee who verifies a digital signature against a valid certificate be a holder in due course of an e-cheque given that section 9 is framed around possession, and what makes such reliance 'without sufficient cause to believe' a defect exists?

3. Do RBI's zero-liability and burden-shifting directions extend to e-cheques and to corporate drawers, and can a regulatory instrument alter the allocation of loss that the statutes suggest?

4. Does Indian law expose a CA to civil liability to a bank or payee who relied on a defective certificate, or is regulation the only sanction?

SCOPE AND LIMITATIONS

The study covers Indian law on e-cheques and the liability of banks, account holders, CAs and holders in due course for cyber fraud. It addresses NI Act, IT Act, RBI directions and precedents. It excludes criminal liability of fraudsters, cross-border jurisdiction, and card, UPI and wallet payments except where decisions on them illuminate general principles.

Limitations: Several recent judgments are known only through secondary reports. Only the abstracts of two journal articles were available that were taken.

RESEARCH METHODOLOGY

The study is doctrinal methodology. It asks what the law is, how it is applied, which suits a question about gaps in existing rules. Primary data, Secondary data and practitioner commentary from journals. Each allocation of loss was tested against three criteria, namely coherence with the statutory scheme, certainty for commercial parties, and whether the loss falls on the party best placed to prevent it. In this case, comparative material was used. An argument from paper cheques to e-cheques is only as strong as the analogy.

DISCUSSION

Does the Forged-Cheque Rule Survive Digital Signatures?

Canara Bank rests on the premise that a cheque is a mandate only if the drawer signed it. A bank paying on a forged signature cannot debit the customer. An e-cheque signed with a stolen private key complicates it, because the signature is technically valid, and a bank will argue that verification discharges its duty of care. The better view is that verification proves integrity and origin of the key, not authority of the person. This follows recent decisions refusing to accept that successful authentication equals authorisation by the customer.16 The RBI supports this by stating that the bank must prove the customer has been negligent for the bank to refuse to reimburse them, and in the 2026 Directions they regard payments made as a result of coercion as fraudulent.17

That analysis fits consumer accounts, but is less clearly correct for corporate accounts--the more likely users of e-cheques, given the instrument's business-to-business origin. 18 The

European Directives assign loss based on authentication and negligence,19 which is consumer-protective. The United States makes a distinction between transfers of funds by consumers under the EFTA and commercial funds transfers governed by Article 4A of the Uniform

Commercial Code. In the latter case, a payment order containing a commercially reasonable security procedure is binding on the customer if the customer does not establish that the fraudulent instruction was not authorized by the organisation or that the fraud was not initiated by third parties accessing the customer’s system.20 India presently has a consumer-style regime and no commercial counterpart. A corporate drawer’s loss therefore falls between the RBI directions (whose application to such drawers is unclear) and Canara Bank, which favours the customer absent estoppel. The coherence criterion is not met.

16 Korde (n 4); ELP (n 4).

17 ELP (n 4).

18 Gopala Krishna and Vidya (n 13).

19 Steennot (n 15); Donnelly (n 16). 20 Steennot (n 15) (EFTA scope); ‘UCC Article 4A Funds Transfers: Protections and Liability’ (LegalClarity, 18 May 2026)

The Account Holder: Section 42 and the Limits of Customer Duty

Section 42 adds something the common law never supply: a lawful duty of reasonable care over a private key and a duty of prompt notice, with liability continuing until notice is given.

Read with section 41(2), which makes the subscriber's certification of key ownership available to all who reasonably rely, the provisions look like a deliberate allocation of risk toward the subscriber in favour of relying parties.

Two features prevent the provision from working as a complete rule. First, it does not state to whom the subscriber is liable or whether liability extends beyond the subscriber's own negligence. Second, the RBI directions wants the bank to prove the customer negligence and treat quick reporting as final.21 The two can be reconciled. Section 42 supplies the standard of conduct (reasonable care and prompt notice), while the RBI directions govern the bank-customer relationship by allocating the burden of proving breach of that standard. A regulatory instrument cannot enlarge a statutory duty, but it can regulate how a bank may claim its benefit.

On this reading the subscriber bears loss only where the bank proves a failure of reasonable care or delay in notice. That fits the listed customer-negligence such as sharing credentials, installing malicious applications, ignoring specific warnings),22 and the urge on vigilance in the

Pallabh Bhowmick case by the Supreme Court.23 It is an interpretation, not a settled rule.

21 ELP (n 4); RBI (n 28).

22 ELP (n 4).

23 Pallabh Bhowmick Case (n 31).

Regulation without a Remedy

The IT Act imposes duties on CAs: to issue certificates only on satisfaction of requirements, to make the section 36 representations, and to suspend or revoke and publish notice. 24 The breaches leads to licensing and penal consequences.27 What the Act does not contain is a clear civil cause of action for a bank or payee who relied on a defective certificate. A claimant would have to use the general provisions on compensation for unauthorised access to computer systems, adjudicated by the statutory adjudicating officer,25 or attempt a claim in negligent misstatement in the manner of Hedley Byrne,26 whose reception for pure economic loss in this setting is untested.

The statutory revocation triggers indicate where a CA's responsibility should lie: issuing to an impostor, or compromise of the CA's own key or security system.27 Those lie within the CA's control; a subscriber's careless key handling or a bank's failure to check certificate status does not. A rule tied to these spheres would satisfy the 'best-placed to prevent' criterion.

The Holder in Due Course

Section 9 describes a holder in due course as a person who, for consideration, becomes the possessor of a cheque payable to the bearer or to the payee or endorsee thereon before the amount becomes payable and without just ground for believing that any defect existed in the title of the person from whom they were taken.28

24 IT 2000 3) ss 35–39.

27IT 2000 3) ss 25, 73.

25 IT Act 2000 (n 3) ss 43, 46.

26 Hedley Byrne & Co Ltd v Heller & Partners Ltd [1964] AC 465 (HL).

27 IT Act 2000 (n 3) s 38(2).

28 NI Act 1881 (n 1) s 9.

Possession and negotiation. The section speaks of a 'possessor', and a transfer that makes the transferee the holder is defined as negotiation.29 The Electronic record has no single physical embodiment; the MLETR treats exclusive control, a reliable method, as the equivalent of possession.30 United States Uniform Commercial Code in its article 12 gives a qualifying purchaser who takes control for value, in good faith and without notice of a claim a position equal to a holder in due course,31 and the United Kingdom has enacted the Electronic Trade

Documents Act 2023. India has no such concept, so a payee's status is uncertain.

Bonafide faith and identifying defect. A Payee verifies the signature, certificate and CA records has stronger basis for claiming good faith.32 Conversely, a payee who ignores a published revocation cannot claim good faith.

Forgery. A title conferred by a forged signature is invalid even on a bona fide taker is a strict rule, as Canara Bank and National Westminster illustrate in the banker-customer relation.33

Whether a cryptographically valid signature created with a stolen key is a 'forgery' is the decisive question, and the statute does not answer it. Two resolutions are possible. If such a signature is treated as forged, every holder is exposed and e-cheques lose commercial value. If it is treated as effective against the world until the subscriber reports compromise, the subscriber (and, after notice, the bank) bears the risk and holders in due course are protected.

Section 42's continuing-liability rule supports the second, and this paper prefers it on the certainty and prevention criteria, subject to the subscriber's rights against the bank where the bank failed in its own duties. This is a normative proposal, not existing law, and it does not touch truncated cheques, where the paper original remains.

29 NI Act 1881 (n 1) ss 8, 9 and 14.

30 Gabriel (n 10).

31 'The UCC Amendments and Their Impact on Negotiable Instruments in Trade Finance' (Mayer Brown, 2023)

32 IT Act 2000 (n 3) ss 39, 41(2).

33 Canara Bank (n 6); National Westminster Bank Ltd v Barclays Bank International Ltd [1975] QB 654.

FINDINGS

Statutory Recognition and Its Incompleteness

The law recognises e-cheques, but it does not clearly cover every part of how they work.

Section 6 includes e-cheques within the meaning of a cheque.34 Section 81A extends the NI

Act to electronic and truncated cheques, with changes that may be made by the Central

Government in consultation with the RBI. 35 However, the rules dealing with negotiation, endorsement and holder in due course still assume that the cheque is physically possessed and delivered. The Act does not clearly explain how these rules apply to electronic cheques.36

Allocation of Duties across the Actors

The account holder or drawer must securely generate the key pair, protect the private key and report any compromise without delay under Sections 40, 41(2) and 42 of the IT Act and relevant

RBI directions. However, the law does not clearly specify the extent of the subscriber's continuing liability. The drawee bank must pay only against a genuine mandate and may claim protection for payment made in due course under Sections 10, 85 and 89 of the Negotiable

Instruments Act, but there is no e-cheque-specific verification standard. The collecting bank is protected under Section 131 of the Negotiable Instruments Act when acting in good faith and without negligence, although the provision is not adapted to electronic presentment. Certifying

Authorities must comply with the IT Act's certification requirements, including suspension or revocation of certificates where necessary, but the law does not expressly establish their civil liability to parties relying on those certificates. Finally, the payee or endorsee may claim the

34 NI 1881 1) s 6.

35 NI 1881 1) s 81A.

36 Na (n 1); see also NI Act 1881 (n 1) s 14.

protection available to a holder in due course under the Negotiable Instruments Act and rely on the subscriber's certification, but the law does not clearly define electronic possession or endorsement. These gaps reveal the absence of a clear, e-cheque-specific framework allocating liability among the parties involved in an electronic cheque transaction. The duty of a

Certifying Authority (CA) to confirm that it has complied with the Act and maintain proper key security.37 The subscriber entitled to use private key after certificate and that the information given to the CA is correct.38 . Under Section 42(1), the subscriber should protect the private key and prevent its disclosure. Section 42(2) requires immediate reporting of any compromise, and the subscriber remains liable until it is reported.39 A CA may revoke the certificate for false material information, failure to meet issuance requirements, or a compromise of its own key or security system affecting reliability, and must publish the suspension or revocation.40

The RBI Framework

RBI's regime has moved from limiting customer liability to imposing positive duties on banks, and the burden of proving customer negligence rests on the bank throughout. The RBI's

Circular dated 6 July 2017 provided zero liability to customers where losses resulted from bank negligence or a third-party breach reported within three working days, while prescribing limited liability in other cases and placing the burden of proof on the bank. The Responsible

Business Conduct Directions, 2025 consolidated these instructions for commercial banks, retaining transaction alerts, 24×7 reporting facilities, reversal timelines and the burden-of-proof rule. Subsequently, the Third Amendment Directions, 2026, dated 24 June 2026, defined

37 IT Act 2000 (n 3) s 36, as summarised in Taxmann, 'Regulation of Certifying Authorities for Cyber Crimes' (Taxmann, 6 February 2024)

38 IT 2000 3) s 41(2).

39 IT 2000 3) s 42; the continuing-liability explanation is noted in Taxmann (n 24).

40 IT 2000 3) ss 38–39.

fraudulent electronic banking transactions, bank negligence, customer negligence and third-party breaches. They provide zero liability for third-party breaches reported within five calendar days, require domestic complaints to be resolved within 45 days, and introduce a one- time compensation of 85% of the net loss, capped at ₹25,000, for eligible individual customers, including sole proprietors, who suffer losses of up to ₹50,000.

None of the descriptions consulted refers to cheques in electronic form, so extension to e-cheques is an inference, not a stated rule.

Judicial Approach

Courts place the risk of unauthorised payment on the bank unless the customer's fault is proved.

The Supreme Court in Canara Bank v Canara Sales Corporation (1987) 2 SCC 666 held that payment made on a forged cheque is unauthorised, as it is made without the customer's mandate. The customer is not required to examine the passbook regularly and is barred from disputing the payment only where their conduct amounts to adoption, ratification or estoppel.

In State Bank of India v Pallabh Bhowmick 2024 SCC OnLine Gau 1519, the Gauhati High

Court addressed fraudulent online debits and the bank's liability, emphasising the importance of timely reporting, customer vigilance and the use of appropriate security technology. Further,

Subodh C Korde 2026 SCC OnLine Bom 3629 and SBI v Prodosh Kumar Banerjee 2026 SCC

OnLine NCDRC 80 reportedly emphasise that the burden of proving customer negligence rests on the bank and that OTP-based authentication alone does not establish that the customer authorised the transaction. These decisions highlight the importance of distinguishing technical authentication from actual customer consent when determining liability for unauthorised electronic transactions. Canara Bank discussed and adopted the English approach in Macmillan and related authority. Confidentiality of OTPs rest on duty of bank and the customers, by the

Pallabh Bhowmick case, decided under the 2017 circular.41

Evidence and Forum

Electronic records now have to satisfy certificate requirement of section 63 of BSA 2023 and replaced the corresponding section 65B of the Evidence Act 1872, but the rulings of the

Supreme court on the older provision are still applicable. Jain cited that the Supreme Court has held that consumer forums cannot deal with fraudulent claims, additionally the Hare Ram Singh verdicts are inconsistent.45

CONCLUSION

The forged-cheque rule in Canara Bank and section 42 of the IT Act pull in different directions and the statute does not reconcile them. The most defensible reconciliation treats section 42 as the standard of customer conduct and the RBI directions as the allocation of the obligation to prove the breach of it. Holder in due course status for an e-cheque is presently uncertain, because section 9 depends on possession and the forged-signature rule is unclear for valid signatures made with stolen keys. The CA's certificate system does supply a workable basis for good faith. The RBI regime is substantively pro-customer and places the burden on the bank, but

it is framed for consumer transactions, is silent on e-cheques, and leaves corporate drawers without an equivalent of the United States commercial security-procedure model. The CA is regulated but not clearly liable, and enforcement is hindered by evidentiary asymmetry and

41 State Bank of India v Pallabh Bhowmick, SLP (C) No 30677 of 2024 (SC, 3 January 2025), reported in Yash Mittal, '"Bank Should Remain Vigilant": Supreme Court Holds SBI Liable to Refund Amount to Customer Who Reported Fraudulent Transaction' (LiveLaw, 6 January 2025) 45Jain (n 19).

forum limits. Conclusions, remains provisional because no reported Indian judgment on e-cheque was found.

SUGGESTIONS

● Restate the negotiation rules for electronic form. The Central Government can use section 81A, in consultation with RBI, to define electronic endorsement and adopt a

'control' test for possession modelled on the MLETR; Parliament should then amend section 9 accordingly.

● Enact an express loss-allocation rule: a subscriber bears loss from misuse of a private key only where he breached section 42 or failed to give notice; after notice the loss falls on the bank; and a holder in due course who verified the certificate and its status takes free of the subscriber's claim.

● Extend the RBI directions to e-cheques expressly and distinguish consumer from commercial drawers. For commercial drawers, an agreed security-procedure model like

Article 4A may be appropriate.

● Create civil liability for CAs for failures within their control (impostor issuance, compromise of the CA's own key, delay in publishing revocation), with liability caps or mandatory insurance.

● Strengthen proof and forums by adopting technical assessors and forensic audit trails, and by requiring banks and CAs to preserve verification logs