INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

ISSN: 2582-6433

November 2026

RESEARCH ARTICLE

Unresolved Liabilities: Legal Accountability in Compromised Digital Tokenisation Systems

Sanjay S

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

Unresolved Liabilities: Legal Accountability in Compromised Digital Tokenisation Systems

Author: Sanjay S

Institution: SASTRA DEEMED UNIVERSITY

Journal: International Journal for Legal Research and Analysis

ISSN: 2582-6433

Unresolved Liabilities: Legal Accountability in Compromised Digital Tokenisation Systems

Sanjay S

SASTRA DEEMED UNIVERSITY

ABSTRACT

With the rapid shift toward digital commerce, traditional credit and debit card storage has been replaced by Card-on-File (CoF) tokenization, where sensitive card numbers are masked with secure cryptographic tokens stored in multi-tiered digital vaults. While this technology helps to secure the front-end, one legal issue arises: If the token vault is compromised, who is legally responsible for the loss?

This research paper examines the inadequacy of existing cyber law frameworks—specifically

Section 79 of the Information Technology Act, 2000 and modern data protection regimes like the DPDP Act, 2023—in addressing multi-party financial data breaches. Section 79 was originally designed to provide "safe harbour" immunity to passive intermediaries hosting third-party content, failing to provide a clear statutory formula for apportioning liability when code-based token infrastructures fail. And Section 43 & 66 penalize hacking and data damage, data theft and security related issues. These provisions struggle to assign multi-party financial liability in complex, automated token systems. Critically, this paper brings out the gaping hole in RBI's tokenization directions which aggressively lays down technical standards, while the

Indian IT Act provides immunity from liability from cyber-crimes, creating a regulatory vacuum between banking related regulations and cyber laws. Thus, there is no clear statutory framework regarding the fixation of liability among the multiparty/multi-tierd chain of parties in a systematic tokenisation breach where, the customer is, who is stuck between multiple corporate giants, become the cyber-victim. Finally, leaving the cardholder to run from pillar to post for compensation.

Keywords: tokenisation; card-on-file; IT Act 2000; Section 79; safe harbour; RBI regulation;

DPDP Act 2023; liability.

INTRODUCTION

Background of the Study

Online merchants once stored full card numbers so that customers could pay with a single click.

This created large databases of card data, and followed by regular breaches. The Reserve Bank of India cautioned about the danger of storing card-on-file data. RBI said that a leak of card-on-file data can cause various problems. It was reported by RBI that customers were compelled by the merchants to save the card details on file.1 Its response was tokenisation, under which the primary account number (PAN) is replaced by the token, and the original number is kept by a Token Service Provider (TSP) that tokenises and de-tokenises.2 The framework began with device-based tokenisation in January 2019, was extended to CoF tokenisation in September 2021, and was implemented from 1 October 2022.3

Tokenisation does not remove risk; it relocates it. A token cannot be breached by a person when token and PAN stays secure, so the vault and de-tokenisation function become the high- value target. In India a token is exclusive to a combination of card, token requestor and merchant, 4 and a single payment may involve the merchant, a payment aggregator, an acquirer, a TSP, and the issuing bank. When the vault fails, the harm falls on a cardholder who dealt with only some of these actors and cannot see the rest.

No single instrument locates liability for such a failure. The Information Technology Act, 2000 offers immunity to middlemen in section 79 and compensation and penal provisions in sections 43, 43A and 66. The Digital Personal Data Protection Act, 2023 lays down security

1Reserve Bank of India, 'Tokenisation of Card Transactions – Enhancements' (Press Release) 2Reserve Bank of India, 'Tokenisation – Card Transactions: Permitting Card-on-File Tokenisation (CoFT) Services' (RBI/2021-22/96, 7 September 2021) 3RBI directs banks to roll out Card-on-File token facility for customers DT Next 4RBI, CoFT Circular (n 2).

requirements for data fiduciaries and is being adopted in stages, with the repeal of section 43A to take effect from May 2027.5 The Supreme court have already applied RBI's customer-protection directions opposing a bank.6 The study matters because consumers need a clear route and proper allocation of liability.

LITERATURE REVIEW

Scholarship relevant to this problem falls into three groups, and none addresses it directly. The gap is therefore filled by reading adjacent literatures together.

The first group asks whether and how law recognises the injury caused by a breach. Solove and Citron argue that courts consistently underestimate the damage caused by violation and that increased risks and anxiety is actually an injury recognized by the law.7 Although their analysis is based on American. If one’s vault is hacked, it does not necessarily mean that all the money has already been withdrawn, and the crucial question is whether the mere fact that card details are available in the dark web qualifies for a Section 43A-type remedy. Romanosky, Hoffman and Acquisti provide additional support for their argument by demonstrating that, more than 230 federal cases, defendants were 30 percent more likely to settle if the plaintiff alleged financial injury or was certified as a class-action.8

The second group views allocation mainly in terms of how it influences incentives. Anderson put-forth that eventhough banks invest less on security, they claim it to be foolproof, instead

5Notification of Digital Personal Data Protection Law in India: Certain Key Timelines (Acuity Law, 2025); Digital Personal Data Protection Act 2023, s 44(2). 6State Bank of India v Pallabh Bhowmick 2024 SCC OnLine Gau 1519: (2025) 1 Gau LR 812: (2025) 1 GLT 337 7Daniel J Solove and Danielle Keats Citron, ‘Risk and Anxiety: A Theory of Data-Breach Harms’ (2018) 8Sasha Romanosky, David Hoffman and Alessandro Acquisti, 'Empirical Analysis of Data Breach Litigation' (2014) better care was given by making the institution responsible.9 Anderson and Moore put it this way: “Security tends to fail when those who can take measures to prevent a harmful outcome don’t pay the cost of doing so”.10 Its limit is that it assumes a bilateral

relationship between institution and customer and does not explain how loss should be shared among several institutions in a chain.

Arun's analysis of gatekeeper liability under Article 19(1)(a) of the Constitution suggests that

Indian intermediary law grew out of concerns over controlling information flow.11 Taking EU,

Keller directs a doctrinal conflict between data protection duties and immunity to intermediary, since these two areas rest on different assumptions.12 Read together, these works suggest that section 79 belongs to a speech-oriented logic and was never calibrated to security duties over financial data. Neither addresses payment infrastructure. This paper tests that suggestion against the text of section 79, the RBI framework and the DPDP Act.

Research Problem

This paper asks whether the intermediary safe harbour in section 79 and the data-security provisions in sections 43, 43A and 66 of the IT Act are legally adequate to apportion liability among the entities in a tokenisation chain when a token vault is breached, given that RBI's mandates and the statutory cyber-liability were not designed to operate together and seems contrary. No instrument allocates loss between the entities, because the cardholder must approach several fora without a clearly identified defendant.

9Ross Anderson, 'Why Cryptosystems Fail' (1994) 10Ross Anderson and Tyler Moore, 'The Economics of Information Security' (2006) 11Chinmayi Arun, ‘Gatekeeper Liability and Article 19(1)(a) of the Constitution of India’ (2014) 12Daphne Keller, 'The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation' (2018)

Research Objectives

(i) To analyse how section 79 and sections 43, 43A and 66 of the IT Act apply to the different actors in a token vault breach;

(ii) To identify the duties that RBI’s tokenisation and customer-protection instruments create, and who bears them;

(iii) To evaluate how the DPDP Act, including the omission of section 43A, changes a cardholder’s prospects of compensation;

(iv) To compare the Indian position with European Union and US method of allocating payment protection loss;

Research Questions

1. To what extent can a TSP or payment aggregator running a token vault satisfy sections

79(1) and 79(2) eventhough by processing, routing and storing credentials rather than merely hosting third party content?

2. What is the criteria for controlling loss allocation among multiple corporate defendants under sections 43, 43A and 66, which govern unauthorised access and negligent data protection in technology & cyber law?

3. Do RBI’s customer-protection directions and the DPDP Act create a genuine conflict with the IT Act, and what legal consequences follow from the distinction?

4. Which features of the EU's PSD2 and GDPR regimes can be transplanted to India, and what adaptation would they need?

SCOPE AND LIMITATIONS OF THE STUDY

Scope: The study covers Indian law. It concerns credit and debit card tokenisation, including card-on-file tokens, and the liability of private entities to each other and to the cardholder. The materials are the IT Act and the Sensitive Personal Data Rules, the DPDP Act and Rules, RBI directions, and precedents. The EU's PSD2 and GDPR which plays a significant or primary role, comparatively with the United States are also dealt.

Limitations: First, the study does not address the criminal liability of attackers, UPI, or non- card tokens. Second, it is non-empirical, so it cannot estimate how often cardholders obtain redress. Third, I found no reported Indian judgment that deals squarely with a token vault breach, so the application of the law is reasoned by analogy from phishing and unauthorised- transaction cases. Fourth, the substantive DPDP provisions are not yet fully in force, so conclusions about them are prospective. Fifth, some details of RBI circulars and DPDP commencement may change from time to time.

RESEARCH METHODOLOGY

This paper adopts doctrinal research. The doctrinal research, identifies and interprets the relevant rules; The comparative part uses the EU and US as reference points to suggest mechanisms that are absent in India.

Data are documentary. Primary sources are statutes (IT Act, DPDP Act, Payment and

Settlement Systems Act 2007, Consumer Protection Act 2019), subordinate legislation, RBI circulars and judicial decisions. Secondary sources are peer-reviewed articles found through searches of journal repositories and publisher sites using terms such as "tokenisation",

"intermediary liability", "safe harbour", "data breach" and "DPDP". Official texts were preferred for primary materials; law-firm commentary was confined only to confirming commencement dates and describing provisions, never as an authority for a legal proposition.

DISCUSSION

1)Absence of clear legal provisions, not a loophole

A common assumption is that the IT Act lets technology companies escape responsibility. The findings refine that claim. Section 79 is not a clear exemption for vault operators; on its text it is poorly matched to their function. The defect is not certain. That uncertainty results in the shifting of a cost onto the less powerful party, and therefore makes predictability impossible, which is crucial for risk apportionment. The same ambiguity clarifies in that both sections 43

and 43A provide grounds for an action, but there is nothing in either one that apportions fault amongst multiple defendants.

2)The law does not clearly address this issue

It is also said that RBI's mandates contradict the IT Act's immunity. On the findings, the more accurate diagnosis is silence. This is an important point when it comes to reform, since if the issue is one of silence, it can be cured by including the recourse rule without abolishing section

79. They collide only in litigation. Suppose an issuer that has refunded its customer sues a TSP and the TSP pleads section 79. The court would need to determine whether RBI's security requirements shape “due diligence” under section 79(2)(c), and whether a regulatory directive can override a statutory immunity. To my knowledge those questions have not been settled for disputes between entities.

3)Who should bear the loss?

Using logic of Anderson and Moore, and Calabresi's principle the loss can be prevented by affordable one and takecare of the responsibility,13 the TSP or vault operator is the natural primary bearer. It controls the keys, the access controls and the de-tokenisation process; the cardholder controls none of these, and the issuer few. In practice the Indian position is the reverse. The first payment is made by the issuer as he is one of the parties in the card user transaction; The under-investment said by Anderson where loss can be passed on, is the reason why it is dangerous. The operator who rarely bears the loss of failure will not have enough incentive to over-invest in security. Fault does not lie only with the operators, a merchant who holds PAN against RBI's guidelines, and the customer who gives away OTP, should also bear some of the loss. The right framework is therefore proportionate, with primary exposure on the operator and contribution rights against others.

4)The cardholder’s path and the 2027 transition

The EU contrast is instructive: PSD2 and the GDPR together guarantee both fast refund and an enforceable compensation right, recourse behind them. India has the refund but not the recourse, and is about to lose the compensation. The main features are the recourse rule, the burden of proof on institution, and joint liability with contribution; It should change to fit India because different bodies such as adjudicating officers, Board and consumer fora overlap.

13Guido Calabresi, The Costs of Accidents: A Legal and Economic Analysis (Yale University Press 1970).

FINDINGS

RBI assigns security roles but not loss

Three RBI instruments define the architecture: the circular of 8 January 2019, the extension circular of 25 August 2021 and the CoFT circular of 7 September 2021. Card networks, and subsequently card issuers, are allowed to serve also as TSPs, while token requestors are directed not to store PANs and explicit customer consent with an additional authentication factor is needed.14 These are duties of conduct. None states who bears the loss when a TSP's vault is compromised. The 2017 customer protection circular stands as the liability allocator, which saves the customer with zero liability when reported within 3 working days for a third- party breach and also transferred the burden of proof on bank.15

Section 79 is textually ill-suited to vault breaches

Section 2(1)(w) includes “online payment sites” within intermediaries and thus an aggregator or TSP may be treated or can claim that status.16 Status alone is not sufficient. Section 79(1) safeguards the intermediary only for liability of self-hosted third-party information, data or links. Section 79(2), protection applies only under certain conditions, does not initiate the transmission, choose the recipient, or alter the information, and also follows the required due

diligence.17 A TSP does the opposite. It generates tokens, transforms card credentials into tokenised data, determines who receives the de-tokenised number, and maintains the related information.

14'Card-on-File Tokenisation Introduced by RBI' (Law.asia); RBI Press Release (n 1). 15Reserve Bank of India, 'Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions' 16Information Technology Act 2000, ss 2(1)(w), 79. 17IT Act (n 17) s 79(2).

First, the cardholder's grievance is that the operator did not protect his/her data under its control, rather than harm arising from third-party content; the loss results from the operator's own actions, which section 79 was not written to excuse. Second, the judicial notice on section 79

concerns knowledge of unlawful content. A court order or government notification alone stands as actual knowledge under section 79(3)b was the decision of Supreme Court in Shreya singhal case,18 and the Delhi High Court held in Myspace that only specific knowledge of infringement is required.19 Since none of the provisions or precedents deal with a security failure, none of them offers a clear decision on whether a payment intermediary can rely on section 79 in reply to a claim of breach. The immunity is not clearly available, but it is not clearly unavailable either.

Sections 43, 43A and 66 give a remedy framed around a single defendant

Section 43 makes a person who accesses or interferes with a computer system without permission liable to pay compensation, and section 43(g) extends this to anyone who assists such access. In ICICI Bank v. Umashankar Sivasubramanian, the Telecom Disputes Settlement and Appellate Tribunal held the bank liable because its negligence contributed to the phishing fraud and also held that one-sided online terms could not be used to avoid statutory liability.20

Under Section 43A, a company may have to pay compensation if it negligently fails to protect sensitive personal data. The 2011 Rules treat card and payment details as sensitive data and recognise IS/ISO/IEC 27001 as a security standard.21 Claims are sent to the adjudicating officers, the jurisdiction of whom under section 46 is limited to ₹5 crore. Since section 66

18Shreya Singhal v Union of India (2015) 5 SCC 1. 19Myspace Inc v Super Cassettes Industries Ltd 2016 SCC OnLine Del 6382. 20ICICI Bank v Umashankar Sivasubramanian Cyber Appeal No 1 of 2010 (TDSAT, 10 January 2019), 2022 SCC OnLine Mad 9500: (2022) 2 LW (Cri) 672: PLR (2022) 208 IJ 11: (2022) 5 LW 414 21Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011, rr 3, 8; IT Act 2000, s 43A.

makes it criminal to carry out dishonest or fraudulent acts in breach of section 43, it applies to the attacker and not to the vault operator unless section 85 assigns the breach to the company.

These provisions give a real remedy, but one built for a single defendant. Where a vault breach involves several body corporates, none of sections 43, 43A or 85 states how fault is divided, whether liability is joint, or how a defendant who has paid may recover from another. Every adjudicating officer must independently decide those questions freshly.

The DPDP Act adds duties without compensation

The DPDP Act requires data fiduciaries to take reasonable security measures under Section

8(5) and report data breaches under Section 8(6). In Section 8(1), the person working behalf is responsible for processors.22 The maximum penalty for failing to protect data is ₹250 crores.23

However, the Act has some gaps for cardholders. The Data Protection Board handles penalties and sends them to the State under section 39, rather than directly to the affected person. The

Act also does not clearly provide compensation to the data principal,24 and section 39 excludes civil-court jurisdiction over matters that the Board can decide. I found no compensation clause for the data principal. Second, From May 2027, Section 44(2) removes Section 43A, which previously provided a basis for compensation for negligent data protection.25 Third, classification is open. The translucent role of a TSP in tokenisation is the followup issue, it might be considered as fiduciary or processor.26 Section 38 gives the DPDP Act priority only where there is an actual conflict with another law.27

22Digital Personal Data Protection Act 2023, ss 8(1), 8(5), 8(6); Digital Personal Data Protection Rules 2025, r 6. 23Digital Personal Data Protection Act 2023, s 33 and Schedule. 24DPDP Act 2023, ss 33, 34, 39. 25'Notification of DPDP Law: Key Timelines' (n 5). 26DPDP Act 2023, ss 2(i), 2(k) and Schedule. 27DPDP Act 2023, s 38.

The merchant has limited RBI regulation, the payment gateway's legal status is unclear, and the card network must follow RBI audits and certification. The card issuer may also operate the token vault. The issuing bank must refund the customer under RBI rules, but cannot clearly recover the loss from other entities. The law does not clearly identify which entity must compensate customers when a token vault is breached.

Courts reason from analogy and leave recovery unanswered

Because no reported decision concerns a token vault, two analogous lines show how courts reason. Under the 2017 circular, SBI had to refund the customer for an unauthorised transaction reported within 24 hours. The Supreme Court noticed that banks can detect such fraud. The same approach in Umashankar, where the first institution bears loss. However, in both cases clearly deals with recovering the loss from other parties.28 The Supreme Court's order was brief and merely disposed of a special leave petition, so I regard it as facts rather than a fully developed precedent.

The EU shows what statutory allocation looks like

Under PSD2, unauthorised payments must generally be refunded by the next working day, with the provider proving authentication and recovering losses from the responsible party.29 Under

GDPR Article 82, the parties does data processing which could be liable for the whole loss, but they can recover their share from others responsible.30 In the US, laws like the EFTA,

28Umashankar (n 21). 29Directive (EU) 2015/2366 on payment services in the internal market [2015] OJ L337/35, arts 72, 73, 92. 30Regulation (EU) 2016/679 [2016] OJ L119/1, art 82(1), (4), (5).

Regulation E, and the Truth in Lending Act limit consumer losses. But for tokenised card payments, who bears the loss mainly depends on card-network rules and contracts.31

Comparative Allocation of Payment-Security Loss (India & EU)

Issue India European Union

Prompt refund, ordinarily by

Customer refund Zero liability for third-party breach if reported within three end of next business day working days (RBI 2017

circular)

On the payment service

Burden of proof On the bank to show customer

negligence

provider

Recourse between

None statutory; contract only Statutory right of recourse institutions

Joint liability for

Not provided in IT Act or

Each controller or processor

liable for whole damage, with

data breach

DPDP Act

contribution

Compensation for

Section 43A until omission;

Right to compensation

none under DPDP Act as

data-breach harm

enacted

31Electronic Fund Transfer Act 15 USC § 1693g; 12 CFR § 1005.6; Truth in Lending Act 15 USC § 1643.

CONCLUSION

Here, the paper set out to test whether section 79 and sections 43 and 66 of the IT Act, read with RBI's mandates and the DPDP Act, can apportion liability among tiered payment entities when a token vault is breached. The answer is that they cannot, but the reason is more specific.

Section 79 is poorly fitted to vault operators and its availability is uncertain. Sections 43 and

43A give a remedy but no method of dividing fault. RBI's instruments protect the customer against the bank but are silent on recovery between institutions The DPDP Act reinforces obligations, yet it eliminates the compensation mechanism found in section 43A and provides no replacement of its own.

It is safe to say that the objective of the research paper has been achieved since the gap has been identified; the problem lies in silence and indeterminacy, not in conflict or loophole. This finding informs the solution, as the gap can be closed through specific rules and does not call for the safe harbour to be dismantled. Two cautions apply: the conclusions on section 79 are interpretive because no case decides the point, and the DPDP Act is still being phased in. For now, a cardholder is protected mainly by the legal exposure of the first institution in the chain under the RBI regulation without a recourse, and that protection thins after May 2027 unless the law changes.

SUGGESTIONS AND FUTURE DIRECTIONS

Suggestions

• The legally mandating rule is needed. Parliament, through an amendment to the payment-systems legislation, or RBI by direction, should provide that an entity which refunds a customer may recover from the entity to which the breach is attributable, modelled on PSD2 article 92.

• Clarify section 79. Ministry of Electronics and Information Technology should clarify, rule or explanatory provision, that entities which tokenise, de-tokenise or store payment credentials act in their own right and cannot invoke section 79(1) against security- failure claims. This eliminates the ambiguity while leaving the safe harbour for content hosting intact.

• Preserve compensation which forms the base. Before section 43A is omitted in May

2027, the government should either defer the omission until a substitute exists or amend the DPDP Act so that the Board can direct compensation to affected data principals.

• Extension of Burden of proof. TSPs should be required to preserve forensic logs and to bear the burden of showing compliance with RBI and DPDP security standards once a vault breach is shown, as PSD2 article 72 does for authentication and the 2017 circular does for banks.

• Role classification. RBI and the Data Protection Board should issue joint guidance on whether TSPs are fiduciaries or processors, so that penalties and contribution rights attach predictably.

• I would state is to practical examination of decisions from adjudicating officer, TDSAT, consumer forum judgment, same as approach of Romanosky and Associates,32 would show how often cardholders recover and from whom. Second, the legal status of RBI directions as a source of enforceable obligations between private entities needs focused doctrinal study. Third, vaultless and network-level tokenisation may change who holds the plot and so who should bear the loss. Fourth, the first Indian vault-breach decision should be analysed against the arguments made here.

32Romanosky, Hoffman and Acquisti (n 9).