*International Journal of Legal Research and Development*
Volume 6 (2026), pages 81–90 e-ISSN 2581-7434

RESEARCH PAPER

# From Leak to Loss: Data Fiduciary Accountability for Downstream Cyber Fraud under the DPDP Act, the IT Act and the Bharatiya Nyaya Sanhita

**G. Uday Kumar**
Independent Researcher

**Article details**

*Published*
28 November 2026
*DOI*
10.5281/zenodo.24629195
*Review*
Peer-reviewed and refereed
*Licence*
CC BY-NC 4.0

**Keywords**
Personal data breach
Cyber fraud
Digital Personal Data Protection Act 2023
Section 43A Information Technology Act
Digital arrest
Victim compensation

**Abstract**

Impersonation frauds in India increasingly depend on personal data that has leaked from the databases of companies and public bodies. Indian law responds to the two ends of this chain separately: the Bharatiya Nyaya Sanhita, 2023 and the Information Technology Act, 2000 punish the fraudster, while the Digital Personal Data Protection Act, 2023 penalises the data fiduciary that failed to protect the data. This paper asks whether the defrauded individual has any effective remedy against the entity whose security failure made the fraud possible. Using doctrinal and analytical methods, it examines the relevant criminal provisions, the security and breach-notification duties under Section 8 of the DPDP Act and the Digital Personal Data Protection Rules, 2025, the penalty and jurisdiction provisions in Sections 33, 34 and 39, and the omission of Section 43A of the IT Act with effect from 13 May 2027. It argues that the new regime fines fiduciaries for the benefit of the State but gives data principals no right to compensation, and that the omission of Section 43A will remove their only statutory claim. Drawing on the Supreme Court's suo motu proceedings on digital arrest scams, in which the Court has required banks to compensate victims where due diligence fails, and on Article 82 of the GDPR, the paper proposes a compensation power, a rebuttable presumption of contribution, a victim fund financed from penalties, and clarification of transitional and jurisdictional questions.

## 1. Introduction

A typical fraud call in India now begins with information the caller should not have: the victim's name, a policy or account number, a recent transaction, or the mobile number linked to an identity document. The fraud itself is only the last link in a chain that often starts elsewhere, in a database that a company or public body failed to protect. Indian law deals with the two ends of this chain separately. Criminal law pursues the person who made the call. Data protection law fines the entity that lost the data. The person who actually lost the money stands outside both processes.

This paper argues that the framework created by the Digital Personal Data Protection Act, 2023 (DPDP Act), as it will operate once its substantive provisions commence, punishes the fraudster and penalises the data fiduciary but does not compensate the defrauded individual.

The omission of Section 43A of the Information Technology Act, 2000 (IT Act) removes the only statutory route by which a person harmed by negligent data security could claim compensation from the entity that held the data. At the same time, the Supreme Court's continuing suo motu proceedings on "digital arrest" scams have begun to build a liability model for banks that, the paper suggests, can be extended in principle to data fiduciaries whose security failures make such frauds possible.

The study is doctrinal and analytical. It examines the relevant provisions of the Bharatiya Nyaya Sanhita, 2023 (BNS), the IT Act, the DPDP Act and the Digital Personal Data Protection Rules, 2025 (DPDP Rules), together with the orders of the Supreme Court and the Madras High Court discussed below. No empirical or field data was collected; figures on cyber fraud are drawn from published reports of official data and are identified as such. Part 2 describes how leaked data feeds fraud. Part 3 examines the criminal law response. Part 4 analyses the DPDP Act's breach regime and its treatment of the individual. Part 5 considers the consequences of omitting Section 43A. Part 6 discusses the judicial response, and Part 7 draws a brief comparison with Article 82 of the European Union's General Data Protection Regulation. Part 8 sets out recommendations.

## 2. The Fraud Pipeline: From Leaked Data to Loss

### 2.1 Why Leaked Data Matters to the Fraudster

Most impersonation frauds depend less on technical skill than on credibility. A caller who claims to be from a bank, an insurer, a courier company or an investigating agency is believed largely because he already knows things about the victim. Leaked personal data supplies exactly that credibility. A name, a phone number and a policy number may each be harmless in isolation; together they allow a stranger to sound like an institution. Generative tools that imitate voices or produce official-looking documents may make such impersonation more convincing, but the underlying raw material remains the personal data itself.

The Star Health episode of 2024 illustrates how such data reaches the open market. In September 2024, the insurer sued the messaging platform Telegram and a self-described hacker after reports that chatbots on the platform were distributing the personal data and medical reports of its policyholders.[1] The Madras High Court granted an interim injunction, and in October 2024 directed the insurer to share the details of the offending bots with Telegram so that the platform could block and delete them, after Telegram stated that it could not search for the leaked material on its own.[2] Notably, the litigation was brought by the company to protect its own interests. The policyholders whose data was exposed were not parties.

[1] 'Star Health Sues Telegram after Hacker Uses App's Chatbots to Leak Data' *Deccan Herald* (Bengaluru, 26 September 2024) <https://www.deccanherald.com/business/companies/star-health-sues-telegram-after-hacker-uses-apps-chatbots-to-leak-data-3207755> accessed 25 November 2026.

[2] 'Madras High Court Directs Telegram to Delete Chatbots Leaking Star Health Insurance Customer Data' *Bar & Bench* (25 October 2024) <https://www.barandbench.com/news/madras-high-court-directs-telegram-delete-chatbots-flagged-star-health-insurance> accessed 25 November 2026; 'Indian Court Tells Star Health to Share Details of Leak so Telegram Can Delete Chatbots' *Insurance Journal* (25 October 2024) <https://www.insurancejournal.com/news/international/2024/10/25/798578.htm> accessed 25 November 2026.

### 2.2 The Scale of the Problem

Official data on cyber fraud, as published through the National Cyber Crime Reporting Portal (NCRP) and reported in the press, shows a sharp rise in impersonation-based frauds. According to an analysis of NCRP data, reported digital arrest incidents rose from 39,925 in 2022 to 123,672 in 2024.[3] Published reports of aggregate fraud losses for 2025 do not agree with one another, and this paper therefore does not rely on any single loss figure. The direction of the trend, however, is not in dispute, and the Supreme Court itself has treated the problem as one of national importance.

### 2.3 The Causation Problem

Any attempt to hold a data fiduciary responsible for a downstream fraud runs into an evidential difficulty. Personal data about an individual is usually held by many entities, and datasets from different leaks are often combined and resold. A victim can rarely prove that the information used against her came from one particular breach. This problem of causation, rather than any lack of moral responsibility, is the main reason why liability tends to stop with the fraudster. Any reform that seeks to bring the data fiduciary into the remedial picture must therefore address causation directly. Part 8 returns to this point.

## 3. Criminal Law: Pursuing the Fraudster

### 3.1 Offences under the Bharatiya Nyaya Sanhita

The BNS, in force from 1 July 2024, contains the general offences under which impersonation frauds are prosecuted. Section 318 defines and punishes cheating (formerly Sections 415, 417, 418 and 420 of the Indian Penal Code, 1860 (IPC)), and Section 318(4), which carries imprisonment of up to seven years and fine, covers cheating that dishonestly induces the delivery of property (formerly Section 420 IPC).[4] Section 319 deals with cheating by personation (formerly Sections 416 and 419 IPC) and carries imprisonment of up to five years.[5] Where the caller pretends to be a police or enforcement officer, as in digital arrest scams, Section 204 on personating a public servant (formerly Section 170 IPC) is also attracted.[6] Threats of arrest used to extract payment may additionally amount to extortion under Section 308 (formerly Sections 383 to 389 IPC).[7] For organised syndicates, Section 111 on organised crime expressly includes cyber-crimes within its scope.[8]

### 3.2 Offences under the Information Technology Act

The IT Act adds offences specific to the digital medium. Section 66C punishes a person who "fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person".[9] Section 66D punishes whoever "by means of any

[3] '#DataViz: How India's Cyber Crime Incidence Is Rising' *IndiaSpend* <https://www.indiaspend.com/data-viz/dataviz-how-indias-cyber-crime-incidence-is-rising-972933> accessed 25 November 2026. The figures are as reported from NCRP data and have not been independently verified against the portal.

[4] Bharatiya Nyaya Sanhita 2023, s 318.

[5] ibid s 319.

[6] ibid s 204.

[7] ibid s 308.

[8] ibid s 111.

[9] Information Technology Act 2000, s 66C.

communication device or computer resource cheats by personation".[10] Each carries imprisonment of up to three years and a fine of up to one lakh rupees. These provisions describe the fraudster's conduct closely, and they are routinely invoked alongside the BNS.

Only one provision is aimed at the leak rather than the fraud. Section 72A punishes a person, including an intermediary, who, while providing services under a lawful contract, secures access to personal information and discloses it without consent, with intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain.[11] The provision reaches the dishonest insider or contractor. It does not reach an organisation that simply failed to secure its systems. Negligent data security, in other words, is not a crime, and the criminal law has no means of treating the leaking institution as a participant in the fraud.

### 3.3 The Limits of the Criminal Route for Victims

Criminal law is designed to punish offenders, not to compensate victims, and its compensatory tools depend on a successful prosecution. A court may order an accused to pay compensation on conviction under Section 395 of the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) (formerly Section 357 of the Code of Criminal Procedure, 1973), and State victim compensation schemes operate under Section 396 BNSS (formerly Section 357A).[12] Where the offenders cannot be traced, where they operate from abroad, or where the money has passed through layers of mule accounts, these remedies offer little. The person who has lost savings therefore looks for a solvent party who can be held liable. The two obvious candidates are the bank through which the money moved and the institution that lost the data. Indian law currently treats these two very differently.

## 4. The DPDP Act: Regulatory Duty without a Private Remedy

### 4.1 The Security and Breach Obligations

The DPDP Act defines a personal data breach to include unauthorised processing and accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to personal data that compromises its confidentiality, integrity or availability.[13] Section 8(5) requires every data fiduciary to protect personal data in its possession or control, including data processed on its behalf by a data processor, by taking "reasonable security safeguards to prevent personal data breach".[14] Section 8(6) requires the fiduciary, in the event of a breach, to inform the Data Protection Board of India (Board) and each affected data principal.[15]

The DPDP Rules, notified on 13 November 2025, give these duties operational content. Rule 6 sets out minimum security measures, and Rule 7 requires a fiduciary to notify affected data principals without delay and to give the Board an initial intimation without delay followed by a detailed report within seventy-two hours of becoming aware of the breach.[16] The obligation

[10] ibid s 66D.
[11] ibid s 72A.
[12] Bharatiya Nagarik Suraksha Sanhita 2023, ss 395–396.
[13] Digital Personal Data Protection Act 2023, s 2(u).
[14] ibid s 8(5).
[15] ibid s 8(6).
[16] Digital Personal Data Protection Rules 2025, GSR 846(E), rr 6–7.

to tell individuals is, for present purposes, the most valuable part of the scheme. A person who knows that her insurer or telecom provider has been breached is better placed to distrust a call that quotes her policy number back to her. Breach notification is therefore a genuine fraud-prevention measure, even though the Act does not describe it in those terms.

These provisions are not yet operative. Under the commencement notification issued on 13 November 2025, Sections 3 to 17 (which include Section 8), Sections 28 to 34 and Section 44(2), among others, come into force eighteen months after publication, that is, on 13 May 2027; Rules 6 and 7 follow the same timetable.[17] Until then, data security in the private sector remains governed by Section 43A of the IT Act and the rules made under it.

### 4.2 Penalties Payable to the State

The Schedule to the DPDP Act authorises penalties of up to two hundred and fifty crore rupees for failure to take reasonable security safeguards and up to two hundred crore rupees for failure to notify a breach.[18] In fixing the amount, the Board must consider factors such as the nature, gravity and duration of the breach, the type of personal data affected, any repetition, and the steps taken to mitigate its effects.[19] These are substantial sums, and they may well improve security practice. But Section 34 directs that all penalties realised by the Board "shall be credited to the Consolidated Fund of India".[20] Not a rupee is earmarked for the people whose data was lost.

### 4.3 Where Is the Individual?

A data principal may complain to the Board about a personal data breach, and the Board may inquire into it.[21] The outcome of such an inquiry is a penalty, a direction or the acceptance of a voluntary undertaking; the Act gives the Board no power to award compensation.[22] The individual is thus cast as an informant rather than as a party with a claim. The Act also imposes duties on data principals, including a duty not to register false or frivolous complaints, and allows the Board to warn or impose costs on such complainants.[23] The asymmetry is striking: the Act contemplates the individual paying for a frivolous complaint but not being paid for a proven breach.

Section 39 deepens the difficulty. It provides that "No civil court shall have the jurisdiction to entertain any suit or proceeding in respect of any matter for which the Board is empowered under the provisions of this Act".[24] Two readings are possible. On a narrow reading, the Board is empowered only to inquire and penalise; compensation is not a matter within its power, so a civil suit for damages in negligence remains open. On a broader reading, the subject matter of the dispute, namely the breach, falls within the Board's remit, and the bar applies regardless of the relief sought. The narrow reading is, in the author's view, more consistent with the principle

[17] Ministry of Electronics and Information Technology, Notification GSR 843(E) (13 November 2025); DPDP Rules (n 16) r 1. Reports from early 2026 described a Ministry proposal to shorten parts of this timeline. At the time of writing, no notification altering the commencement dates has been located, and the position should be re-checked before publication.
[18] DPDP Act (n 13) sch, items 1–2.
[19] ibid s 33(2).
[20] ibid s 34.
[21] ibid s 27(1)(b).
[22] ibid ss 28, 32–33.
[23] ibid ss 15, 28.
[24] ibid s 39.

that provisions ousting the jurisdiction of civil courts are construed strictly, but the question has not yet been decided and remains genuinely open. A similar uncertainty surrounds complaints of deficiency in service before consumer commissions.

The absence of a compensation remedy was a deliberate legislative choice. The Committee of Experts chaired by Justice B.N. Srikrishna recommended a compensation framework, and the Personal Data Protection Bill, 2019 carried this forward in Clause 64, which empowered an adjudicating officer to award compensation to data principals.[25] That clause did not survive into the 2023 Act, which replaced the compensation model with a penalty model.[26]

## 5. Section 43A and the Remedial Vacuum

### 5.1 What Section 43A Offers Today

Section 43A makes a body corporate that possesses, deals with or handles sensitive personal data or information in a computer resource it owns, controls or operates, and that is negligent in implementing and maintaining reasonable security practices, liable to pay damages by way of compensation to the person affected, where the negligence causes wrongful loss or wrongful gain.[27] Claims of up to five crore rupees are decided by an adjudicating officer, and larger claims by a competent court.[28] The provision has clear limits: it applies only to bodies corporate and only to the categories of data the 2011 Rules treat as sensitive. Yet those categories include passwords and financial information, which are precisely the kinds of data that fraudsters exploit. For a fraud victim, Section 43A is an imperfect but real remedy.

### 5.2 The Omission and Its Transitional Effect

Section 44(2)(a) of the DPDP Act omits Section 43A, and Section 44(2)(c) omits the rule-making power under which the 2011 Rules were framed.[29] The omission takes effect with the eighteen-month tranche on 13 May 2027.[30] Whether claims arising from breaches that occur before that date survive is a question of transitional law. The Supreme Court has held that the omission of a provision is to be treated as a repeal for the purposes of Section 6 of the General Clauses Act, 1897, which preserves rights and liabilities accrued under the repealed law unless a different intention appears.[31] On that reasoning, a Section 43A claim relating to a breach before 13 May 2027 should remain enforceable after the omission. The DPDP Act contains no saving clause either way, and an express clarification would remove doubt.

[25] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians* (Ministry of Electronics and Information Technology 2018); Personal Data Protection Bill 2019 (Bill No 373 of 2019), cl 64.

[26] Vaishnavi Viswanathan, Davis Kanjamala and Viswanathan G, 'The Hollow Heart of Data Protection: How the DPDP Act Abandons the Data Breach Victim' *Bar & Bench* <https://www.barandbench.com/view-point/the-hollow-heart-of-data-protection-how-the-dpdp-act-abandons-the-data-breach-victim> accessed 25 November 2026.

[27] IT Act (n 9) s 43A; Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[28] IT Act (n 9) s 46.

[29] DPDP Act (n 13) s 44(2).

[30] GSR 843(E) (n 17); Taxmann, 'SPDI Rules and the DPDP Act – What Changes' <https://www.taxmann.com/post/blog/spdi-rules-vs-dpdp-act> accessed 25 November 2026.

[31] *Fibre Boards (P) Ltd v Commissioner of Income Tax* (2015) 10 SCC 333.

### 5.3 After May 2027

For breaches occurring after the omission, the victim of a leak-driven fraud will have no statutory claim for compensation against the entity that lost the data. What remains is the common law of negligence, assuming Section 39 does not bar it. A negligence claim requires the claimant to establish a duty of care, a breach, and damage caused by that breach. Each element is difficult in the data context, and causation, for the reasons given in Part 2, is often fatal. The practical result is that the law will move from a regime in which a limited compensation claim existed to one in which, for most victims, it does not.

## 6. The Judicial Response

### 6.1 The Digital Arrest Proceedings

On 17 October 2025, the Supreme Court took suo motu cognisance of digital arrest scams on a complaint from a senior citizen couple from Ambala, Haryana, who had been defrauded of more than a crore of rupees by persons posing as investigating officers and using forged orders bearing the name of the Court.[32] On 1 December 2025, a Bench of Chief Justice Surya Kant and Justice Joymalya Bagchi directed that the Central Bureau of Investigation would be the primary agency to investigate digital arrest cases.[33] On 4 August 2026, the Court directed the Reserve Bank of India (RBI) to adopt a standard operating procedure for banks and asked an inter-departmental committee to examine a framework for shared liability and victim compensation.[34]

The most significant development came on 29 October 2026. A Bench of the Chief Justice, Justice Joymalya Bagchi and Justice V. Mohana observed that the regulatory measures proposed by the RBI must require financial institutions to indemnify victims of digital arrest and other cyber frauds, with compensation not less than the amount lost, where the fraud occurred because the institution failed to exercise due diligence.[35]

The reasoning behind this direction deserves attention. The Court places liability on the institution that controlled a point at which the fraud could have been stopped, and makes that liability turn on a failure of due diligence rather than on proof that the institution intended or knew of the fraud. The same reasoning applies, with at least equal force, to a data fiduciary. The fiduciary controls the security of the data that made the fraud credible, and Section 8(5) already defines the standard of care it must meet. If due-diligence failure is a sound basis for requiring a

[32] *In Re: Victims of Digital Arrest Related to Forged Documents*, SMW (Crl) No 3 of 2025 (SC, order of 17 October 2025); 'Supreme Court Seeks Response from All States, UTs on "Digital Arrest" Scams; Mulls CBI Probe' *The Leaflet* <https://theleaflet.in/leaflet-reports/supreme-court-seeks-response-from-all-states-uts-on-digital-arrest-scams-mulls-cbi-probe> accessed 25 November 2026.

[33] *In Re: Victims of Digital Arrest* (n 32) (order of 1 December 2025); Anmol Kaur Bawa, 'Supreme Court Directs CBI to Investigate Digital Arrest Scam Cases, Asks States to Give Consent' *LiveLaw* (1 December 2025) <https://www.livelaw.in/top-stories/supreme-court-directs-cbi-to-investigate-digital-arrest-scam-cases-asks-states-to-give-consent-311774> accessed 25 November 2026.

[34] *In Re: Victims of Digital Arrest* (n 32) (order of 4 August 2026); Amisha Shrivastava, 'Digital Arrest Scams: Supreme Court Issues Directions for Prevention, Compensation & Grievance Redressal' *LiveLaw* (4 August 2026) <https://www.livelaw.in/top-stories/digital-arrest-scams-supreme-court-issues-directions-for-prevention-compensation-greivance-redressal-544292> accessed 25 November 2026.

[35] *In Re: Victims of Digital Arrest* (n 32) (order of 29 October 2026); Saket Sourav, 'Digital Arrest Scam Victims Must Get Compensation Equal to Loss if Banks Fail Due Diligence: SC' *Law Street* (11 November 2026) <https://lawstreet.co/judiciary/digital-arrest-scam-victims-must-get-compensation-equal-to-loss-if-banks-fail-due-diligence-sc> accessed 25 November 2026.

bank to compensate, a proven failure of reasonable security safeguards is a comparable basis for requiring a data fiduciary to contribute. Two caveats must be stated. First, the Court's orders are directions in a continuing suo motu proceeding addressed to the RBI and the banking system; they do not themselves create a general rule of liability for other entities. Secondly, extending the principle to data fiduciaries would require legislation or regulation, not merely judicial analogy.

### 6.2 The Banking Framework and Its Gap

The RBI's 2017 circular on limiting customer liability already provides for zero customer liability in cases of third-party breach, where the deficiency lies neither with the bank nor the customer but elsewhere in the system, provided the customer reports the unauthorised transaction promptly.[36] This might appear to cover leak-driven fraud, but it does not. The circular is concerned with unauthorised transactions, whereas in impersonation and digital arrest frauds the victim is usually manipulated into authorising the payment herself. In the author's reading, such a transaction falls largely outside the circular, and where the customer is treated as having shared credentials, the circular places the loss on the customer until the matter is reported. The Supreme Court's due-diligence approach fills part of this gap for banks, but neither instrument reaches the institution whose leak supplied the fraudster with the victim's details.

### 6.3 Litigation over Leaks

The *Star Health* proceedings show the other side of the judicial picture. Once a leak occurs, the relief that courts are asked to grant is directed at containment, such as blocking and deleting the leaked material, and it is sought by the fiduciary to protect its own reputation and business.[37] Takedown orders are necessary, but they do nothing for the policyholder who has already received a fraudulent call. The legal system is thus well equipped to protect the data holder after a leak and poorly equipped to compensate the data subject.

## 7. A Comparative Note: Article 82 of the GDPR

The European Union's approach shows that regulatory penalties and individual compensation can coexist. Article 82 of the General Data Protection Regulation gives any person who has suffered material or non-material damage as a result of an infringement a right to compensation from the controller or processor.[38] The Court of Justice has held that a mere infringement does not by itself give rise to compensation; actual damage must be shown, though there is no threshold of seriousness.[39] In a case arising from a cyberattack on a public authority, it further held that unauthorised disclosure by third parties does not by itself prove that the controller's measures were inadequate, that the controller bears the burden of proving that its security measures were appropriate, and that a data subject's fear of possible misuse of her data can itself amount to non-material damage.[40]

[36] 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, 6 July 2017) para 6.
[37] *Bar & Bench* (n 2); *Insurance Journal* (n 2).
[38] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [2016] OJ L119/1, art 82(1).
[39] Case C-300/21 *UI v Österreichische Post AG* EU:C:2023:370.
[40] Case C-340/21 *VB v Natsionalna agentsia za prihodite* EU:C:2023:986.

Two lessons follow for India. The first is that a compensation remedy need not be unlimited or speculative; the requirement of proven damage keeps it within bounds. The second, and more important, is that placing the burden of proving adequate security on the controller goes a long way towards solving the causation and evidence problem identified in Part 2. The data fiduciary, not the victim, knows what safeguards it had in place. European law is not a template to be copied wholesale, and Indian conditions, including the volume of potential claims and the capacity of adjudicating bodies, differ significantly. But the structural point transfers well.

## 8. Recommendations

The analysis above supports the following reforms, set out in order of priority.

**First**, Parliament should amend the DPDP Act to empower the Board, or a designated adjudicating officer, to award compensation to data principals who suffer loss from a breach of Section 8(5), drawing on the model of Clause 64 of the 2019 Bill. Without such a power, the Act protects data as a regulatory object but not the people to whom it relates.

**Secondly**, any compensation provision should include a rebuttable presumption. Where the Board has found a failure of reasonable security safeguards, and the victim shows that a fraud against her used data of the kind exposed in that breach within a reasonable period afterwards, the fiduciary's contribution to the loss should be presumed unless it proves otherwise. This addresses causation without imposing liability for every fraud on every fiduciary.

**Thirdly**, Section 34 should be amended so that a defined share of penalties collected for security and breach-notification failures is credited to a fund for victims of cyber fraud, administered alongside the victim compensation schemes under Section 396 BNSS. This would give victims some recourse even where the specific source of the leak cannot be identified.

**Fourthly**, the scope of Section 39 should be clarified to confirm that civil courts and consumer commissions retain jurisdiction over claims for compensation, since the Board has no power to grant that relief.

**Fifthly**, the Central Government should clarify by notification or amendment that Section 43A claims relating to breaches occurring before 13 May 2027 survive the omission of that provision.

**Sixthly**, breach notifications under Rule 7 should be shared, in appropriate form, with the Indian Cyber Crime Coordination Centre and the banking system, so that accounts and customers exposed in a major leak can be monitored for suspicious activity. This would link the DPDP regime to the fraud-prevention framework the Supreme Court is building for banks.

## 9. Conclusion

India is assembling three separate responses to leak-driven fraud: criminal liability for the fraudster, regulatory penalties for the data fiduciary, and, through the Supreme Court's intervention, a due-diligence liability for banks. What is missing is a link between the entity whose failure exposed the data and the person who paid for that failure. The omission of Section 43A in May 2027 will widen that gap at exactly the moment when the DPDP Act is supposed to strengthen individual protection. The eighteen-month transition period offers an opportunity

to correct this before the new regime takes full effect. A data protection law that measures its success by the penalties it collects, rather than by the harm it prevents and repairs, will remain incomplete. The defrauded data principal should be at the centre of that law, not on its margins.

---

**How to cite this paper:** G. Uday Kumar, 'From Leak to Loss: Data Fiduciary Accountability for Downstream Cyber Fraud under the DPDP Act, the IT Act and the Bharatiya Nyaya Sanhita' (2026) 6 International Journal of Legal Research and Development 81.