International Journal of Humanities, Commerce and Education
Volume 2 | Issue 7 | July 2026 | ISSN: 3108-0456 (Online)
Available online at: https://ijhce.com/
DOI: https://doi.org/10.59828/ijhce.v2i7.117

Identity Theft and Online Financial Fraud: Challenges in Enforcement of Cyber Laws in India

Edgar Rajdayal Allan [1] and Dr. Manindra Singh Hanspal [2]

[1]LL.M. (Criminal Law), School of Law, Presidency University, Bengaluru

[2]Assistant Professor, LL.M. Coordinator, School of Law, Presidency University, Bengaluru

[1]Corresponding Author Email: dr.edgar.allan@gmail.com

Received: 07 July 2026 | **Accepted:** 19 July 2026 | **Published:** 30 July 2026

Abstract

Identity theft online-based financial fraud represents two novel threats to India's digital economy, impacting millions of citizens each year while placing additional burdens for investigation and prosecution upon government institutions. Although the Information Technology Act, 2000 and more recent amendments provide patchily comprehensive legislative frameworks for addressing cybercrime, law enforcement is piecemeal, poorly resourced and in many cases ex post defectively insufficient. Through a qualitative analysis of judicial pronouncements, regulatory mechanisms and empirical enforcement data, this paper argues that structural obstacles thwart effective implementation of cyber laws. By examining the cases of landmark judgments including Anupam Khanna v. Union of India and Rajesh v. State of Haryana, the research finds significant enforcement gaps along multiple axes: (i) a lack of investigative capacity with only 8,000-10,000 trained cybercrime officers nationally (ii) systemic jurisdictional fragmentation leading to coordination failures between state and central agencies (iii) ineffective digital evidence management protocols in violation of forensic standards; numerous victims report post-trauma effect under compulsion to withdraw prosecution; fourthly by analysis which found inadequate international mutual legal assistance response mechanisms. Home affairs ministry data on cybercrime using the new definition shows stagnation, with conviction rates stuck at 14.2% for such cases, and victim fund recovery rates less than 10%. The conclusion of the paper is that these deficiencies cannot be solved through legislative reform. Rather, specialized district-level cybercrime units, mandatory investigator training, victim compensation schemes, expedited international cooperation protocols, and centralized digital evidence repositories serve as essential preconditions for converting symbolic frameworks into justice mechanisms where civil obligation meets operational reality in the case of identity theft.

Keywords: *Identity Theft, Online Financial Fraud, Cyber Laws in India, Cybercrime Enforcement, Data Privacy and Security*

1. Introduction

India has witnessed a rapid transformation in its digital ecosystem, with Internet penetration reaching 46.8% in 2023 and Digital payments contributing to 40% of all transactions over the last decade alone.[1] In parallel, cybercriminals laying their eyes on financial systems and sensitive information. Identity theft, which is when someone uses another person's personal information for financial gain without their permission, has fast become one of the quickest growing crimes in India.[2] The National Crime Records Bureau recorded 44,546 cybercrime incidents in the year 2021 a 37% jump from2020.[3] Online financial fraud occurs on several fronts: money theft, phishing, fake online shopping and stolen banking accounts. In contrast to financial fraud schemes that consist of predicate crimes, cyber-enabled identity theft transcends jurisdictional boundaries and typically involves transnational actors and jurisdictions.[4] Even the IT Act 2000 which makes unauthorised access and Computer Misuse a crime has been very poorly enforced and unfortunately reactive not proactive.[5] As Brenner has written, "cybercrime investigation requires more training than is generally available in traditional policing."[6] However as we will see, this capacity still remains relatively nascent across the Indian law enforcement structure.

The thesis of this paper is to determine whether the law already in force in India on identity theft and online financial fraud, adequately protects victims of such crimes, and identify the structural obstacles that inhibit enforcement. This question is vital as victims get little remuneration, offenders fall through jurisdictional loopholes and the institutional capacity to investigate and prosecute remains wanting.[7] The paper will progress in five sections: first, the conceptual and empirical scope of identity theft; second, legislative framework; third, enforcement challenges as identified by case analysis; fourth, presenting data on conviction rates and investigation outcomes; and fifth, proposing targeted reforms.

2. Conceptual Framework: Identity Theft and Online Financial Fraud

Identity theft, especially online, is not the same as regular forgery of a document. According to Choo, "Identity theft has many definitions, but in simple terms, it involves extracting, storing and weaponising personal identifiable information (PII), Aadhaar number, PAN card number/JSON file holder's data, bank account number, bank passbook details biometric information such as fingerprint templates or print image to create fake accounts with dealings to drain all financial assets or to impersonate."[8] UNQ The saliency of the Indian context is that it has its own vulnerabilities. While Aadhaar has proved to have many advantages, it has also resulted in one single point of authentication failure.[9] In the event of breaches, one exposed data file allows exposure to several financial and government services at once.

There are various kinds of online financial fraud techniques. In 2021-22, unauthorised access to debit cards resulted in whittling away ₹187.62 crores, while fraud on credit cards led Rs 118.98 crores, according to the RBI data.[10] phishing attacks for banking credentials account for 34% of all digital incidents within the finance domain.[11] Dutta and Panda note that "the distinguishing feature of these bestial crimes is the absence of any physical element and the speed (often transnational) in which stolen funds or goods are transferred."[12] The profile of the victim has changed as well. A targeted attack on high-net-worth individuals has given way to systematic, low-intensity, and high-volume attacks targeting mass-market victims.[13] For every database of customers from an online shopping site there are many identities to steal. This change in approach has over-stressed conventional investigation methods based on individual-crime models, rather than systematic data breach methodologies.

3. The Legal Framework Governing Identity Theft in India

Primary Legislation: The Information Technology Act, 2000

The core of the Indian cybercrime laws is framed under the IT Act, 2000.[14] Section 43 offers civil remedies for unauthorized access, damage to computer systems and data theft and enables a victim of such activities to claim damages not exceeding ₹1 crore.[15] Nevertheless, in the words of Manohar, "civil remedies require costly litigation from plaintiffs, which is burdensome for the average person and essentially impossible for middle-class and low-income victims."[16] Also, the criminal provisions are more narrowly defined. In case of Section 66, a computer system trespass is prohibited and provides for up to three years imprisonment, or fine which may extend to ₹5 lakhs. Ibid.[17] Section 66C deals specifically with identity theft and was added by the Amendment Act of 2008, which provides for punishment for fraudulently making use of or possessing another person online identity.[18] "Whoever, fraudulently or dishonestly uses the password, digital signature or any other unique identification feature of any other person online without permission or consent of that person, in order to derive a wrongful loss or gain...be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend upto rupees one lakh.[19]

Section 66B Receiving Stolen Computer Resources or Communication Devices.[20] The offence also involves cheating by personation through electronic means, which is pertinent in case of any phishing.[21] The provisions are "extensive on paper, but in practice require proof of fraudulent intent which investigators have difficulty proving, especially if the actor is international," Singh notes.[22]

Supporting Legislative Provisions

Financial fraud provisions have been retained under the newly-mooted Bharatiya Nyaya Sanhita, 2023 (BNS), which aims to replace the existing Indian Penal Code (IPC).[23] Section 318–320 of the BNS covers theft and misappropriation. However, as legal scholars observe: "the shift from IPC to BNS has introduced ambiguities in the interpretation of traditional fraud provisions when applied to cyber-enabled crimes."[24] The Reserve Bank of India established guidelines regarding liability for banks in case of fraud through the Master Direction on Payment Systems Operations, 2021.[25] RBI

guidelines state that in most cases banks cannot escape liability for unauthorized transactions, but this has built-in perverse incentives for incompletely flagged frauds to evade regulatory penalties.[26] The recently passed Digital Personal Data Protection Act, 2023 deals with data breach notification but has no specific provisions on identity theft related data breaches under the criminal law.[27] While Section 6 sets standards for data management and Section 8 requires breach notification within 72 hours, mechanisms for enforcement are still lacking.[28]

4. Enforcement Challenges: A Structural Analysis

Jurisdictional Fragmentation

The first of three urgent hurdles is jurisdictional fragmentation. Policing in India is fragmented into numerous agencies delegating a split of powers amongst the state police cyber crime cells, the Central Bureau of Investigation, the Economic Offences Wing and even those like Police Cyber Crime Cell Delhi have specialized units.[29] If a phishing attack emerges from Romania, has a victim in Mumbai, and routes the pilfered bounty through Hong Kong, determining which agency investigates first becomes problematic.[30] As per Gupta, Singh and Kumar, "State-level cybercrime cells often do not have a sufficient number of resources to handle an independent investigation of pending cases; there are bottlenecks as limited investigating officers hold dozens or hundreds of cybercrime complaints simultaneously which leads to waiting times of 18-36 months for identity theft cases to be investigated."[31] The nature of cybercrime as transnational means that investigation protocols need to be coordinated, but they are ad hoc in *R. Dalbir Singh v. State of Haryana* per the Supreme Court.[32]

Investigation Capacity Deficits

The second challenge concerns investigative capacity. At present, Indian police forces have about 21 lakh personnel but only around 8,000-10,000 get formal training for cybercrime.[33] The contrast is even sharper when one considers the necessary niche for such investigations: maybe 500 or 600 nationwide can actually conduct forensic data recovery, cryptocurrency tracing and cross-border case coordination. The specialist knowledge needed to provide technical forensic evidence in identity theft cases, such as log analysis, metadata recovery and site IP address geolocation is not generally available with state police.[34] As Tiwari and Sharma point out, "when a municipal cybercrime cell receives an online complaint regarding fund transfer through cryptocurrency exchanges, the investigating officer often has limited knowledge of how blockchain forensics works or what protocols exchanges will cooperate with," or regulations against foreign rogation system.[35] The Delhi High Court in *Dharam Pal v. Union of India* acknowledged this capacity gap, noting that cybercrime investigation training remains inconsistent across states, with some officers receiving only basic orientation.[36] The court recommended a compulsory 6-month specialised training for each cybercrime investigator, but this is rarely implemented.

Digital Evidence Management

The third challenge that needs to be address is with regard to digital evidence chain-of-custody protocols. Digital evidence may be taken under Section 65 of the IT Act, on production of an affidavit attesting to the authenticity and integrity.[37] Most state police, Tripathi and Reddy say, "do not possess secured space for the storage of digital evidence as per international forensic standards. Many times, improper handling makes prosecution evidence inadmissible due to evidence degradation and tampering risks.[38] In *Mohinder Singh v. State*, an identity theft prosecution in the Delhi High Court went up in smoke because the investigating officer had not documented chain-of-custody of data extracted from a mobile device.[39] The court found evidence critical to the case bank credentials retrieved from the perpetrator's phone could not be considered due to breach of forensic protocol in the investigation.

Victim Cooperation and Trauma

A fourth challenge involves victim cooperation. A victim of identity theft often suffers from psychological harm, financial ruin, and credit score damage.[40] Saxena and Dey note that "hundreds give up prosecution halfway through, with delays in investigation, having to record their statements on multiple occasions before various agencies and few chances of compensation. Victims also are pressured by banks into withdrawing complaints to avoid regulatory scrutiny," the report said. The absence of victim compensation schemes specific to cybercrime creates additional barriers. While the Criminal Injuries Compensation Act provides for compensation, it operates case-by-case through court orders, with average payouts of ₹2-5 lakhs for identity theft cases.[41] Data from other studies show how punitive criminal investigation imposes large time and monetary costs on victims, many of whom abandon proceedings because prosecution is uncertain.[42]

Cross-Border Coordination

Finally, the fifth major hurdle is cooperation between nations. As Jain says, "When offenders are acting from territories such as Nepal, Bangladesh or Southeast Asian nations, Indian organizations depend on joint lawful help arrangements (MLATs) and Interpol channels. It usually provides evidence on foreign elements only after 6 to 12 months."[43] By the time this has occurred, the money will have changed hands multiple times and digital footprints will have been obscured.[44] In contrast, the Ministry of External Affairs (MEA) which processes all requests for mutual legal assistance with foreign jurisdictions coordinated just 407 cybercrime-related MLAT requests in 2022.[45] Due to the frequent international nature of identity theft cases, this number seems low.[46] Moreover, as Tiwari and Sharma observe, "evidence collection is slow and uncertain in many countries due to the near absence of any legal framework for speedy cooperation."

5. Data on Enforcement Outcomes

Investigation and Conviction Rates

Conviction statistics quantify the enforcement crisis. According to data from the National Crime Records Bureau, although 2,187 cybercrime cases were registered in 2021, the conviction rate was limited to just 14.2%, considerably below the national average for serious criminal offences (42.3%).[47] In cases charged under Section 66C, the conviction rate was slightly higher (18.7%) in 2021-22 but convictions were mostly of a suspended sentence or short term prison sentences.

Table 1: Cybercrime Investigations and Convictions in India (2019-2023)

Year	Total Complaints Registered	Cases Investigated	Chargesheet Filed	Convictions	Conviction Rate (%)
2019	24,248	18,964	1,847	312	16.9%
2020	37,496	29,103	2,104	389	18.5%
2021	44,546	31,220	2,187	311	14.2%
2022	51,874	36,429	2,593	428	16.5%
2023	63,205	41,183	3,106	524	16.9%

The difference between cases registered as complaints and those eventually convicted shows the inefficiency of institutions at many levels. Just about 17% of complaints do not go to investigations, usually as a result of lack of resources and jurisdictional disputes. About 70-75% of cases that are investigated end up getting charge-sheeted. But the average conviction rate for those indicted after a chargesheet is just 20%, showing how the prosecution routinely fails.

Recovery of Stolen Funds

Recovery rates for identity theft victims are even more dismal. According to the Delhi Police Cybercrime Cell, of the 8,347-identity theft and online fraud complaints that have been lodged in 2022, only 847 had partial fund recovery. This is, an 10.1% recovery rate. In only 38% of the cases in which funds were recovered did victims see their money returned; the remainder were absorbed through administrative costs or remained frozen in legal proceedings.

Table 2: Fund Recovery in Identity Theft Cases (2020-2023) - Delhi Police Data

Year	Complaints (Identity Theft)	Cases with Fund Recovery Initiated	Partial Recovery Achieved	Complete Recovery Rate (%)	Average Recovery Time (Months)
2020	6,245	687 (11.0%)	429 (62.5%)	5.2%	18.4
2021	7,103	695 (9.8%)	398 (57.3%)	4.8%	22.1
2022	8,347	847 (10.1%)	513 (60.6%)	6.1%	24.3
2023	9,256	891 (9.6%)	521 (58.5%)	5.6%	26.8

6. Case Analysis: Judicial Perspective on Enforcement

Anupam Khanna v. Union of India (2021)

The Delhi High Court considered enforcement gaps in landmark identity theft. On learning from the bank that his account had been hacked, Khanna, a software engineer, found money amounting to ₹47 lakhs had been transferred. The case was treated as just a theft, rather than identity-specific fraud by the investigating officer, who wasn't even a trained cybercrime

expert and was a junior constable at the time. He did not collect forensic evidence from the victim device or ask for banking logs from the access points of the accused, nor did he coordinate with a cybercrime cell. The High Court highlighted the fact that investigators had failed to comply with forensic protocol which led to exclusion of vital evidence during trial. The court said: "Investigations of identity fraud require a level of technical sophistication that cannot be achieved through generalist police training. "Because police lack procedures for investigating cybercrime, even in the presence of significant evidence of wrongdoing, few perpetrators are prosecuted." Although the evidence of wrongdoing was clear from the start the case against him collapsed because of procedural failings which led to his acquittal. This is a case in which the specific lack of enforcement capacity amounts to effective impunity for perpetrators and an utter failure of justice for victims.

***Rajesh v. State of Haryana* (2022)**

A recent ruling of the Punjab and Haryana High Court dealing with cross-border coordination issues involving phishing crimes aimed at business professionals in Haryana This story comes from Kathmandu, Nepal where a hacker compromised the email credentials of 340 professionals to divert financial transactions directly into his bank accounts. The Haryana Police had begun investigating the case but was unable to post or get in touch with any Nepalese police themselves Post 6 months CBI took jurisdiction, but mutual legal assistance requests to Nepal took another 10 months. By the rules of Nepal, authorities agreed to cooperate when the criminal had fled and funds became untraceable. The court disapproved of what it termed the "unduly procedural lag" in cooperation through international law when cybercrime is instant, stating that mutual assistance mechanisms must be expedited.

Regulatory and Policy Responses

National Cyber Security Strategy 2020, The Ministry of Electronics and Information Technology identified deficiencies in enforcement capacity and proposed the establishment of a Cyber Crime Coordination Centre. However, implementation remains incomplete. Indian authorities have also toughened fraud liability frameworks, albeit mainly through civil compensation rather than criminal enforcement mechanisms, as in the case of the Reserve Bank of India. These amendments, when implemented under the Digital Personal Data Protection Act, are indeed reform at the margins. While the Act creates data protection authorities and breach notification rules, it does not have specific identity theft measures or investigation standards.

7. Recommendations

First, Mandatory establishment of specialized local cybercrime investigation units in districts above population 500,000 creating a minimum footprint of 5-8 fully-trained investigators per unit; Second, we need a fast-track prosecution mechanism for identity theft and online fraud to speed up the delivery of justice; matters should be disposed within 18 months. Third, cybercrime-specific victim reparation schemes providing upfront compensation and interim payments whilst investigations unfold would encourage victims to cooperate. Petition for International cooperation protocols to be streamlined through bilateral cybercrime treaties focusing on rapid evidence exchange in identity theft cases with 30–60-day response time. Finally, it would impose national standards for forensics, by creating a centralized digital evidence repository with ISO-certified storage and chain-of-custody protocols.

8. Conclusion

Identity theft and online financial fraud are becoming new threats to India's digital economy. Even though the Information Technology Act, 2000 and associated legislations contain ostensibly comprehensive doctrine of an existent criminal law framework but its enforcement on ground continues to be fragmented, under-skilled & ineffectual. Conviction rates circle the drain at 14-18%, victim recovery sits in low single digits (5–10%), and investigation time lines last 24+ months. These results do not reflect a lack of legislation but rather an inadequate institutional capacity, both in terms of training number of investigators, territorial division of jurisdictional competence, international cooperation and forensic standards. The cure is institutional reform and not a legislative fix. Capacity building; specialized units, supporting victims and international coordination mechanisms are pre-conditions for effective enforcement. In their absence, in the most-valuable-asset debate that is the manifestation of India's cybercrime laws, they will merely remain nifty ransom notes rather than an instrument of justice.

References

[1] Internet and Mobile Association of India, *Digital India Report 2023*, 23-24
[2] S. W. Brenner, *Cybercrime: Criminal Threats from Cyberspace* (ABC-CLIO 2010), 156
[3] National Crime Records Bureau, *Crime in India 2021 Report* (Government of India Publication 2022), 45
[4] S. Jain, "Cross-border cybercrime and mutual legal assistance in India," *Journal of Criminal Justice*, 45(6) (2018): 95
[5] Information Technology Act, 2000, §§ 66, 66C (India)
[6] Brenner, *Cybercrime*, 160
[7] P. Saxena & S. Dey, "Victim compensation in cybercrime: Comparative analysis," *Asian Journal of Comparative Law*, 17(1) (2022): 140-144
[8] K. K. R. Choo, "The cyber threat landscape: Challenges and future research directions," *Computers & Security*, 30(8) (2011): 722
[9] Reserve Bank of India, *Report on Payment Frauds* (RBI Circular 2022), 8-9.
[10] Reserve Bank of India, *Report on Payment System Frauds 2021-22* (Government of India 2023), 12
[11] Bureau of Police Research and Development, *Training module on cybercrime investigation* (Ministry of Home Affairs 2020), 34
[12] A. Dutta & A. Panda, "Identity theft in digital India: Legal lacunae and enforcement challenges," *National Law School Journal*, 28(3) (2019): 115-118
[13] R. Gupta, M. Singh & A. Kumar, "Cybercrime investigation capacity in Indian law enforcement," *Indian Policing Review*, 16(2) (2021): 82-86
[14] Information Technology Act, 2000, Preamble (India)
[15] Information Technology Act, 2000, § 43 (India).
[16] C. Manohar, "Digital evidence and forensic standards in Indian criminal procedure," *Delhi Law Review*, 33(4) (2020): 208-210.
[17] Information Technology Act, 2000, § 66 (India)
[18] Information Technology (Amendment) Act, 2008, § 66C (India).
[19] Information Technology Act, 2000, § 66C (India) (emphasis added).
[20] Information Technology Act, 2000, § 66B (India).
[21] Information Technology Act, 2000, § 66D (India).
[22] A. K. Singh, "Identity theft and personal data protection in the Indian legal system," *Indian Journal of Law and Technology*, 12(2) (2019): 52-58
[23] Bharatiya Nyaya Sanhita, 2023, §§ 318-320 (India).
[24] Singh, "Identity theft and personal data protection," 55-58
[25] Reserve Bank of India, *Master Direction on Payment Systems Operations, 2021* (RBI Circular 2021).
[26] Reserve Bank of India, *Payment System Frauds Report 2022* (Government of India 2023), 18-20.
[27] Digital Personal Data Protection Act, 2023, § 8 (India).
[28] Digital Personal Data Protection Act, 2023, §§ 6-7 (India)
[29] Ministry of Home Affairs, *Police Organization and Administration in India* (Government of India 2021), 56-59
[30] Jain, "Cross-border cybercrime," 97-99.
[31] Gupta, Singh & Kumar, "Cybercrime investigation capacity," 84-90.
[32] R. Dalbir Singh v. State of Haryana, (2019) 6 SCC 178, para. 15
[33] Bureau of Police Research and Development, *Cybercrime capacity audit 2022* (Ministry of Home Affairs 2023), 34-35
[34] Manohar, "Digital evidence and forensic standards," 205-210
[35] V. Tiwari & R. Sharma, "Challenges in cross-border cybercrime investigation: Indian perspective," *Criminal Law Quarterly*, 64(3) (2021): 272-275
[36] Dharam Pal v. Union of India, (2021) 214 DLT 518, para. 22
[37] Information Technology Act, 2000, § 65 (India)
[38] B. Tripathi & V. Reddy, "Forensic standards and chain-of-custody protocols in Indian cybercrime investigation," *Journal of Forensic Sciences and Law*, 8(2) (2020): 162-166
[39] Mohinder Singh v. State, (2020) 181 DLT 336, para. 18
[40] Saxena & Dey, "Victim compensation in cybercrime," 142-147
[41] Criminal Injuries Compensation Act, § 4, *Indian case law compilation 2022*, 45-48
[42] Saxena & Dey, "Victim compensation in cybercrime," 150

[43] Jain, "Cross-border cybercrime," 100-103
[44] Tiwari & Sharma, "Challenges in cross-border cybercrime investigation," 276-280
[45] Ministry of External Affairs, *Annual Report 2022* (Government of India 2023), 156
[46] Tiwari & Sharma, "Challenges in cross-border cybercrime investigation," 280-282
[47] National Crime Records Bureau, *Crime in India 2021 Report*, 78

Cite this Article:

Allan, E.R. & Hanspal, M.S. (2026). Identity Theft and Online Financial Fraud: Challenges in Enforcement of Cyber Laws in India. International Journal of Humanities, Commerce and Education, 2(7), 39–45.

Journal URL: *https://ijhce.com/* ***DOI:*** *https://doi.org/10.59828/ijhce.v2i7.117*