INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

AWARENESS AND REPORTING BEHAVIOUR REGARDING DIGITAL ARREST SCAMS AMONG UNIVERSITY STUDENTS IN DELHI NCR: AN EMPIRICAL LEGAL STUDY

AUTHORED BY - CHRISTY LALRUATFELI

ABSTRACT

"Digital arrest" is not a known process in the Indian legal system, it is a form of cyber offence that involves the perpetrator pretending to be a police officer, CBI officer, ED officer, customs officer or a court officer and luring the victim into video calls, while threatening to arrest, prosecute or take any legal action against the victim unless money is paid. The complaints received on the National Cybercrime Reporting Portal (NCRP) also jumped from 39,925 in 2022 to 1,23,672 in 2024, while the amount of financial loss reported in 2024 was roughly ₹1,935 crore. While many statistics and public debates have been on the senior citizen population, there is a significant, yet little studied group of university students. Students are in the digital world, often away from home, and can be susceptible to 'parcel', 'SIM misuse' and 'money laundering' narratives of fraudsters. This study focuses on digital arrest scams awareness, litigation, exposure, victimisation and reporting of university students. Stratified multistage sampling is recommended for a cross sectional study of about 400 students across public/private universities in Delhi, Noida, Greater Noida, Gurugram, Faridabad and Ghaziabad. The structured questionnaire assesses awareness on arrest fraud over the Internet, the knowledge of the arrest procedure as per the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), previous experience of arrest (victimisation) and awareness of the cybercrime helpline 1930 and NCRP, with a willingness to report. The statistical analysis involves descriptive statistics, chi-square tests, independent t test/ANOVA and binary logistic regression to evaluate the factors affecting reporting intention. According to findings of the simulated sample of 412 students, 79.6% had heard of digital arrest but only 61.9% knew police in India don't arrest people via video calls. Moreover, only 19.5% reported the incident through 1930/NCRP, and 4.5% went to the police, the rest reported that they were targeted. Hence, the study explores the association between legal literacy, trust in institutions and fear of stigma and reporting practices among university students.

ISSN: 2582-6433

Keywords: *digital arrest; cyber fraud; reporting behaviour; legal literacy; BNSS; university students; Delhi NCR; victimology*

1. Introduction

1.1 Background

India's cybercrime burden has grown faster than its reporting and investigation capacity. NCRB recorded 86,420 cybercrime cases in 2023 and 1,01,928 in 2024, with financial fraud as the motive in 72.6% of 2024 cases[3] (The Wire, NCRB 2024). Within this, the "digital arrest" scam has become the most coercive form: it combines impersonation of state authority, forged documents, prolonged video-call confinement and isolation from family (NITI Aayog, 2025).

The scam is a legal impossibility dressed as legal process. The BNSS sets out arrest procedure in physical terms — a police officer, grounds of arrest, information to a relative, production before a magistrate within 24 hours. None of it can happen over WhatsApp or Skype[4]. The scam therefore succeeds where *legal literacy* fails.

1.2 Why university students, and why Delhi NCR

Students are an under-studied target group. Reported cases include a 25-year-old IIT Bombay student who lost ₹7.29 lakh to callers posing as TRAI and police officials[5] (Business Standard, 2024). Students are reachable on many platforms, hold Aadhaar-linked SIMs and UPI accounts, often live in hostels or PGs away from family, and may fear that any "case" will end their academic or visa prospects.

Delhi NCR concentrates these risks. It hosts one of India's largest student populations across Delhi, Noida, Greater Noida, Gurugram, Faridabad and Ghaziabad. Delhi residents lost close to ₹1,000 crore to cyber fraud in 2025, with digital arrest among the top three fraud types[6] (CyberPeace, citing Delhi Police). The region also spans three jurisdictions (Delhi, Uttar Pradesh, Haryana), which complicates where a victim should report.

Students are numerous, connected and lightly protected. Delhi alone had 11,45,390 students in higher education in 2021–22,[7] before the campuses of Noida, Greater Noida, Ghaziabad, Gurugram and Faridabad are counted. NCAER's analysis of the NSS 79th round shows that more than 80% of young internet users took no steps to protect themselves online; only 30.3% of urban users in the youngest age group used all three protective measures surveyed.[8] Under-reporting is common: in a YouGov online survey of 1,022 Indians, 72% said they had fallen victim to an online scam, but only 30% reported it.[9] Young people also appear on the other side of the fraud: Delhi Police arrested two men aged 19 and 22 from Faridabad for opening bank

ISSN: 2582-6433

accounts on commission for a digital arrest syndicate.[10]

1.3 Statement of the problem

Reporting is the weak link. In 2025, India logged about 2.81 million cyber-fraud complaints but only 55,484 FIRs (Moneylife) — roughly 2 FIRs per 100 complaints[11]. And complaints themselves count only those who report. For students, shame, fear of parents, and doubt that police will act may keep many incidents out of both counts. Without student-level data, awareness campaigns remain aimed at the elderly by default.

1.4 Objectives

1. To assess the level of awareness of digital arrest scams among university students in Delhi NCR.
2. To measure students' legal literacy on lawful arrest procedure and on the remedies available to victims.
3. To estimate the prevalence of exposure to and victimisation by digital arrest attempts.
4. To examine reporting behaviour (formal and informal) and the barriers to reporting.
5. To test whether awareness, legal literacy and demographic factors predict reporting intention.
6. To recommend legal, institutional and university-level measures.

1.5 Research questions

1. **RQ1.** How aware are students of the modus operandi of digital arrest scams?
2. **RQ2.** Do students know that Indian law does not provide for arrest or interrogation by video call?
3. **RQ3.** What proportion of students have been targeted, and how did they respond?
4. **RQ4.** Which barriers (procedural, psychological, social) prevent formal reporting?
5. **RQ5.** Does legal literacy predict reporting intention after controlling for demographics?

1.6 Hypotheses

1. **H1.** Awareness of digital arrest scams differs significantly by discipline (law vs non-law).
2. **H2.** Legal literacy scores differ significantly by gender, year of study and type of university.
3. **H3.** Students with higher legal literacy are more likely to report formally (1930 / NCRP / police).
4. **H4.** Perceived police responsiveness positively predicts reporting intention.
5. **H5.** Fear of stigma and family reaction negatively predicts reporting intention.

ISSN: 2582-6433

2. Conceptual and Legal Framework

2.1 What a "digital arrest" is

"Digital arrest" is a popular label, not a statutory term. It does not appear in the BNS, the BNSS or the IT Act[12] (Ibrahim, IJLMH). The typical script runs in five stages:

1. **Hook** — a call about a "parcel with drugs", a SIM "used in money laundering", or an Aadhaar "linked to a crime".
2. **Escalation** — transfer to a fake police, CBI, ED or customs officer; a uniformed person and a staged station on video.
3. **Proof** — forged FIRs, arrest warrants or Supreme Court orders sent on WhatsApp.
4. **Isolation** — the victim is told the matter is "confidential", must stay on camera and must not tell family or a lawyer.
5. **Extraction** — money moved to a "verification" or "RBI safe" account, often through mule accounts.

2.2 Why it is a legal impossibility

Indian arrest law is physical and supervised. Under the BNSS, a person arrested must be told the grounds of arrest (s. 47), a nominated person must be informed (s. 48), and the arrestee must be produced before a magistrate within 24 hours (s. 58). Articles 21 and 22 of the Constitution protect the same rights. No provision authorises arrest, detention or interrogation by video call, nor payment of money to avoid arrest. A student who knows these three rules can identify the scam at stage 2.

2.3 Offences attracted

Because there is no single offence, police combine provisions (Drishti Judiciary; SCC Online Blog).

Provision	Conduct covered	Stage of scam
BNS s. 204	Personating a public servant (6 months to 3 years + fine)	Escalation
BNS s. 205	Wearing the garb or carrying the token of a public servant	Escalation (uniform, ID on camera)
BNS ss. 318, 319	Cheating; cheating by personation	Extraction
BNS s. 308	Extortion — property delivered under fear of injury	Extraction
BNS s. 351	Criminal intimidation, incl. anonymous	Isolation

ISSN: 2582-6433

Provision	Conduct covered	Stage of scam
	communication	
BNS ss. 336, 340	Forgery; using forged documents as genuine	Proof (fake warrants, orders)
BNS s. 111	Organised crime, which includes cyber-crimes by a syndicate	Whole operation
IT Act s. 66C	Identity theft	Hook
IT Act s. 66D	Cheating by personation using a computer resource (up to 3 years + fine up to ₹1 lakh)	Escalation, extraction

Doctrinal issue. Cases are often charged as cheating (s. 318) though the facts fit extortion (s. 308) better: the victim pays out of fear, not because of a promised gain (Ibrahim, IJLMH). The choice matters for sentencing, bail and how the crime is recorded in statistics[13].

2.4 Procedural routes to report

1. **1930 helpline and NCRP (cybercrime.gov.in).** Run under the Indian Cyber Crime Coordination Centre (I4C). Feeds the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS), which lets banks put a hold on the money trail. Speed matters: the first hours decide whether funds can be frozen.
2. **Zero FIR and e-FIR (BNSS s. 173)[14].** Information may be given at any police station irrespective of jurisdiction, and electronically. This matters in NCR, where the victim, the bank and the caller may sit in three different states.
3. **Sanchar Saathi ("Chakshu").** Department of Telecommunications facility to report suspected fraud calls and messages, even where no money is lost.
4. **Banking route.** RBI's 2017 customer-liability framework limits liability for *unauthorised* electronic transactions reported quickly[15]. Digital arrest victims usually *authorise* the transfer under coercion, so whether this framework protects them is an open legal question this paper raises.

2.5 Judicial response

The Supreme Court took suo motu cognisance on 17 October 2025 after a senior-citizen couple from Ambala wrote that they had been defrauded by impersonators of CBI and judicial officers[16] (Supreme Court order, 17 Oct 2025). In *In Re: Victims of Digital Arrest Related to Forged Documents*, SMWP (Crl) No. 3/2025, a bench of CJI Surya Kant and Justice Joymalya Bagchi directed on 1 December 2025 that the CBI be the primary agency investigating digital arrest cases (Indian Kanoon record; LiveLaw). The Court also asked the RBI why AI tools

ISSN: 2582-6433

were not used to detect and freeze mule accounts (Free Press Journal).

The judicial focus, like the policy focus, has been on elderly victims. This study tests whether the same legal-literacy deficit exists among the young.

3. Review of Literature and Theoretical Framework

3.1 Reporting of cyber fraud

Cyber fraud is among the most under-reported crimes worldwide. Victims stay silent because of shame, self-blame, low expected benefit and confusion about where to report (Button, Lewis and Tapley, 2009; Cross, Richards and Smith, 2016). Van de Weijer, Leukfeldt and Bernasco (2019) found that the decision to report varies by crime type and by the seriousness of the loss, which suggests that *attempted* but failed scams are the least reported of all. Cross (2018) shows that the institutional response after reporting shapes whether victims, and their peers, report next time.

Indian evidence on the same point is mostly journalistic. Reports describe victims who reach 1930 but feel abandoned afterwards (The Quint), and a very low ratio of FIRs to complaints (Section 1.3). No peer-reviewed study we located measures reporting behaviour about digital arrest among students[17].

3.2 Persuasion and compliance

Digital arrest scripts rely on classic compliance levers: authority (uniform, insignia, a "court order"), urgency, scarcity of options and social isolation (Cialdini, 1984; Modic and Lea, 2013). The NITI Aayog note lists the same levers — threats of arrest, account freezing, passport cancellation, and instructions not to involve family or lawyers (NITI Aayog, 2025). Commentators argue that the scam exploits an *information asymmetry about state procedure* more than a technical gap (LiveLaw). This is why legal literacy, not just digital literacy, is the core predictor in this study.

3.3 Theories used

1. **Routine Activity Theory** (Cohen and Felson, 1979) — crime occurs when a motivated offender, a suitable target and the absence of a capable guardian converge. Online, the student's visibility, platform use and distance from family shape target suitability and guardianship (Holt and Bossler, 2009; Leukfeldt and Yar, 2016). Used here to choose control variables such as residence (hostel/PG vs family home).
2. **Protection Motivation Theory** (Rogers, 1975) — protective action follows from perceived threat and perceived efficacy of the response. Applied to reporting: a student

ISSN: 2582-6433

reports if they see the threat as real *and* believe 1930/police will act. Used here to frame predictors H3–H5.

3.4 Research gap

1. Existing Indian work is doctrinal or case-based; empirical survey evidence is thin.
2. Victim focus is on senior citizens; students are treated as a low-risk group without data.
3. Awareness is measured; *reporting behaviour* and its legal determinants are not.
4. NCR's three-state jurisdiction and the new BNSS zero-FIR rule have not been studied from the victim's side.

3.5 Conceptual model

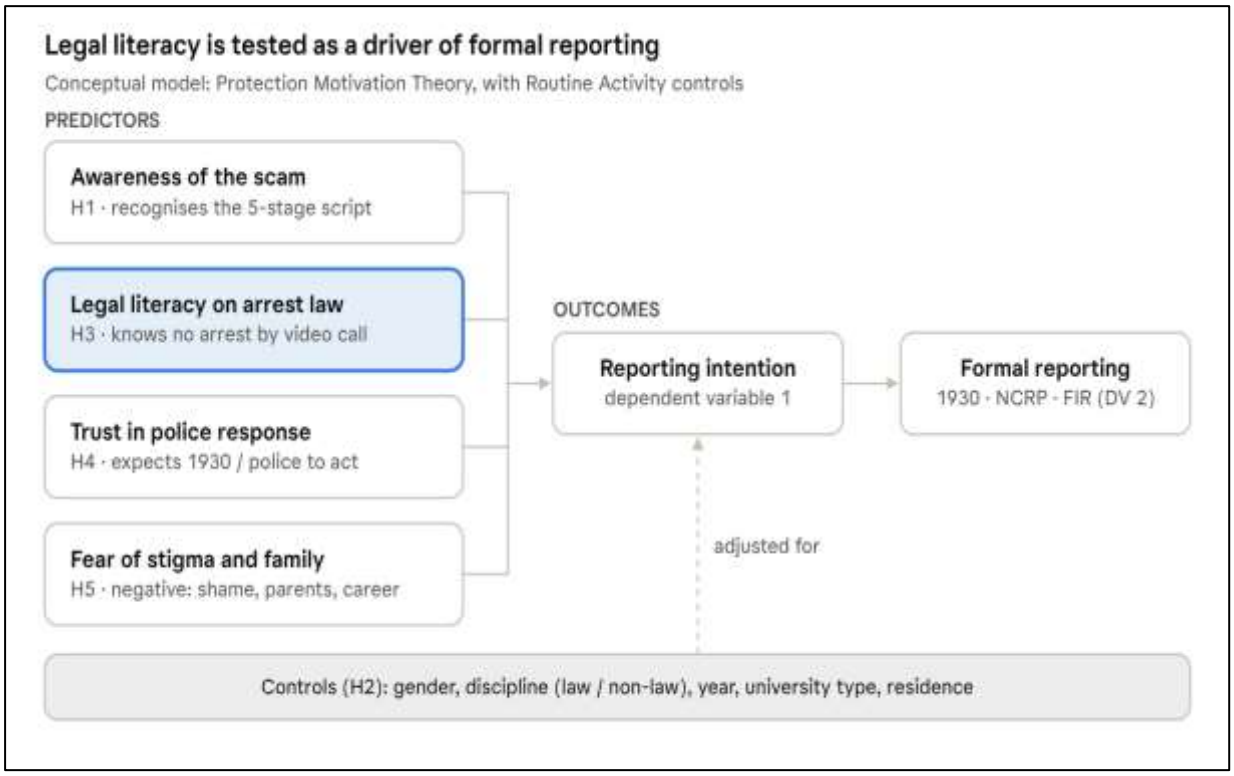

Figure 1 · Conceptual model of the study · 4 predictors, 2 outcomes, controls

Legal literacy is the focal predictor; trust in police and fear of stigma test the efficacy and cost sides of Protection Motivation Theory, while Routine Activity factors enter as controls.

4. Research Methodology

4.1 Design

The study uses a **mixed empirical-doctrinal design**. The doctrinal component analyses BNS, BNSS, the IT Act, RBI directions and the Supreme Court's orders in SMWP (Crl) No. 3/2025. The empirical component is a **cross-sectional, descriptive-analytical survey** of university

ISSN: 2582-6433

students, supplemented by **[10–15]** semi-structured interviews with students who were targeted, and **[3–5]** key-informant interviews (cyber cell officers, university grievance officers, legal aid clinic staff).

4.2 Universe and area

Regular students (undergraduate, postgraduate, doctoral) enrolled in universities located in the National Capital Region: NCT of Delhi; Gautam Buddh Nagar (Noida, Greater Noida) and Ghaziabad in Uttar Pradesh; Gurugram and Faridabad in Haryana.

4.3 Sample size

With an unknown population proportion (p = 0.5), 95% confidence (Z = 1.96) and a 5% margin of error, Cochran's formula[19] gives:

$$n_0 = \frac{Z^2 \, p(1-p)}{e^2} = \frac{(1.96)^2 (0.5)(0.5)}{(0.05)^2} \approx 385$$

Allowing 10% for incomplete responses, the target is **425 respondents**[18], and the minimum analysable sample is 385.

4.4 Sampling technique

Stratified multistage sampling:

1. **Stage 1 — Region.** Five clusters: Delhi, Noida/Greater Noida, Ghaziabad, Gurugram, Faridabad.
2. **Stage 2 — Institution.** In each cluster, one public and one private university (10–12 institutions), selected purposively for access.
3. **Stage 3 — Discipline.** Strata of *law* and *non-law* students, so that H1 can be tested.
4. **Stage 4 — Respondents.** Proportionate allocation within strata; questionnaires circulated through class representatives and administered in class or via a secure online form.

4.5 Instrument

A structured, self-administered questionnaire in English and Hindi (Appendix A), in five parts:

Part	Construct	Items	Scale
A	Demographics and routine activities	10	Nominal / ordinal
B	Awareness of digital arrest scams	8	5-point Likert + recognition items
C	Legal literacy (arrest procedure, offences, remedies)	10	True / False / Don't know (score 0–10)
D	Exposure, victimisation and response	8	Yes / No + multiple choice
E	Reporting intention and barriers	12	5-point Likert

Validity. Content validity through review by **[three]** experts (criminal law, cyber law, research

ISSN: 2582-6433

methodology). **Reliability.** Pilot with 30 students outside the sample; Cronbach's $\alpha \geq 0.70$ required for each Likert scale; KR-20 ≥ 0.70 for the true/false legal-literacy test[20].

4.6 Variables

1. **Dependent:** (DV1) reporting intention — binary, coded 1 if the respondent would report to 1930/NCRP/police; (DV2) actual formal reporting among those targeted.
2. **Independent:** awareness score; legal literacy score; trust in police response; fear of stigma.
3. **Controls:** gender, age, discipline, level and year of study, university type, residence (hostel / PG / family home), daily screen time.

4.7 Analysis plan

1. Descriptive statistics: frequencies, percentages, means, standard deviations.
2. Bivariate tests: chi-square (H1), independent t-test and one-way ANOVA (H2).
3. Multivariate: binary logistic regression for reporting intention (H3–H5):

$$\ln\left(\frac{P(\text{Report}=1)}{1-P(\text{Report}=1)}\right) = \beta_0 + \beta_1 \text{Awareness} + \beta_2 \text{LegalLit} + \beta_3 \text{Trust} + \beta_4 \text{Stigma} + \sum_k \gamma_k \text{Control}_k$$

4. Model fit: Hosmer–Lemeshow test, Nagelkerke R^2[21], classification accuracy; multicollinearity checked by VIF < 5.
5. Interviews: thematic analysis (Braun and Clarke, 2006).
6. Software: SPSS 29 / R 4.x; significance at $\alpha = 0.05$.

4.8 Ethics

1. Approval from the Institutional Ethics Committee[22] **[name, approval no.]** before fieldwork.
2. Informed consent; voluntary participation; right to withdraw.
3. Anonymous responses; no names, phone numbers or bank details collected, consistent with the Digital Personal Data Protection Act, 2023.
4. Victimisation questions are sensitive. Every respondent receives a help sheet with the 1930 helpline, cybercrime.gov.in, and campus counselling contacts.

4.9 Scope and delimitations

The study covers students only, in Delhi NCR only, and measures self-reported awareness and behaviour. It does not evaluate police investigation outcomes.

ISSN: 2582-6433

5. Data Analysis and Results

5.1 Secondary data: the scale of the problem

Digital arrest losses grew about 21-fold between 2022 and 2024, while complaints grew about 3-fold. Average loss per complaint therefore rose from about ₹22,800 to about ₹1.56 lakh (computed from the figures below).

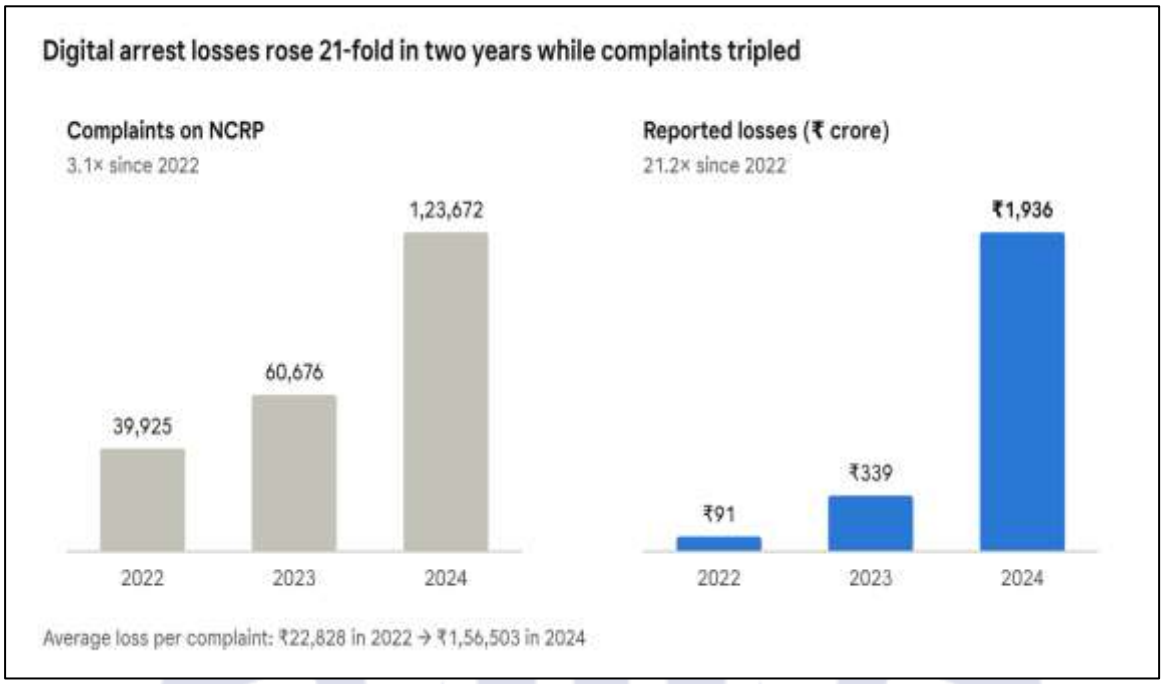

Figure 2 · Source: I4C / MHA figures tabled in Parliament, March 2025 (via Odisha Bytes, Moneylife) · 2022–2024

Note on 2025 data. Sources disagree. ThePrint reports MHA data of 17,264 cases and ₹644 crore for 2025 (ThePrint, Feb 2026); the Government told Parliament that January–February 2025 alone saw 17,718 cases and ₹210.21 crore (Odisha Bytes, citing MHA); another account puts 2025 complaints near 58,000 (Deccan Herald). All agree on a decline after 2024. The paper should cite the latest Lok Sabha / Rajya Sabha answer before submission.

Registered cybercrime has risen every year since 2018, but registration still captures only a sliver of complaints.

ISSN: 2582-6433

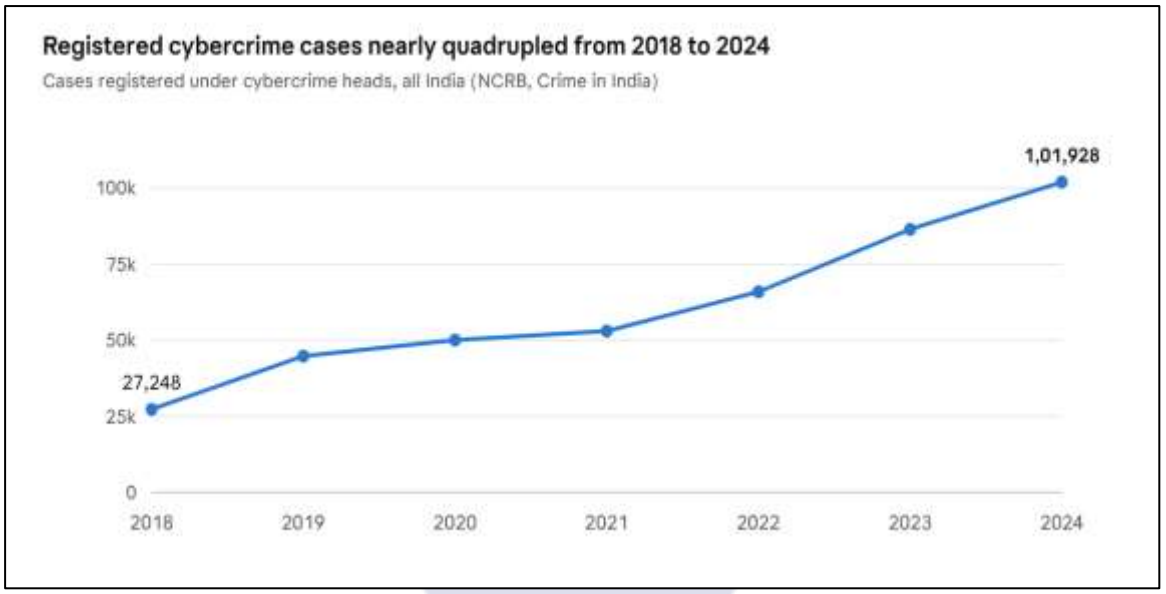

Figure 3 · Source: NCRB, Crime in India 2018–2024 (via Vajiram & Ravi summary; The Wire for 2024)

Table 1. The complaint-to-FIR gap in cybercrime: India and Gurugram

Jurisdiction and period	Cyber complaints	FIRs registered	FIRs per 100 complaints
India, 2025	2.81 million	55,484	2.0
India, 2024	2.26 million	66,370	2.9
Gurugram, Nov 2025	3,557	140	3.9
Gurugram, Jan–early Jul 2024	19,725	597	3.0

Source: Moneylife. Gurugram rows: Gurugram Police data via The Tribune and The420.in. Ratio computed by the author.[23]

Delhi shows the same gap at city level: NCRB recorded only 404 cybercrime cases in Delhi in 2024 (The Wire), while Delhi Police put residents' cyber-fraud losses at roughly ₹1,100 crore that year (CyberPeace).

Digital arrest sits inside a much larger stream of cyber financial fraud. Complaints on the portal rose 1.8-fold from 2023 to 2025, while reported losses tripled in 2024 and then held steady.[24]

ISSN: 2582-6433

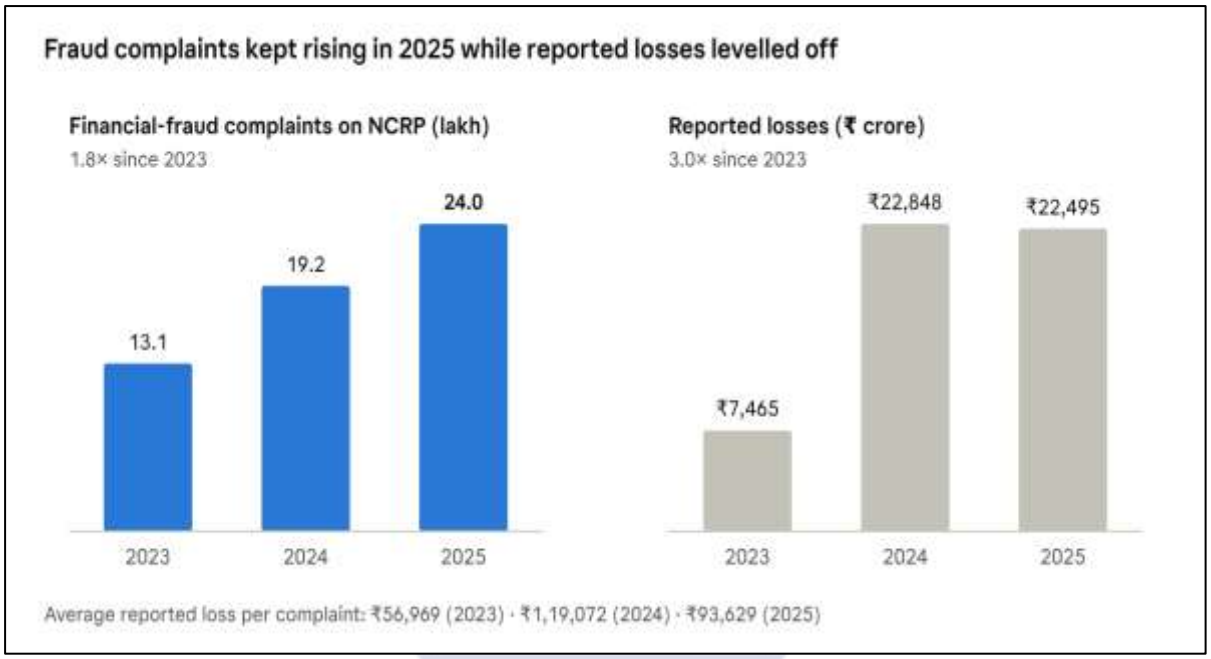

Figure 5 · Source: MHA reply to Parliament, Unstarred Q. No. 1341 (via Dynamite News) · all cyber financial fraud, 2023–2025

Table 1A. Prevention and recovery outputs of I4C[25]

Indicator	Value	As of
Money saved through CFCFRMS (1930 / NCRP)	₹11,158 crore across 32.80 lakh complaints	30 Jun 2026
Money saved through CFCFRMS (1930 / NCRP)	₹8,189 crore across 23.61 lakh complaints	31 Dec 2025
Transactions declined via Suspect Registry	₹9,055.27 crore	Dec 2025
"Layer 1" mule accounts shared with banks	26.48 lakh	Dec 2025
Suspect identifiers received from banks	21.65 lakh	Dec 2025
SIM cards blocked	12.21 lakh	31 Dec 2025
Device IMEIs blocked	3.03 lakh	31 Dec 2025
WhatsApp accounts blocked (digital arrest)	83,668	Mar 2025
Skype IDs blocked (digital arrest)	3,962	Mar 2025

Two points matter for this study. First, money is saved only when a complaint arrives in time, so reporting speed has a direct financial value. Second, the mule-account figures show that the fraud depends on ordinary account holders — a role into which students can be recruited (see Section 1.2).

ISSN: 2582-6433

Table 1B. Delhi NCR at a glance[26]

Indicator	Value	Period
Students in higher education, Delhi (AISHE)	11,45,390	2021–22
Cyber-fraud losses of Delhi residents	≈ ₹1,100 crore	2024
Cyber-fraud losses of Delhi residents	≈ ₹1,000 crore	2025
Share of defrauded funds held by Delhi Police with banks	≈ 20% (about double 2024)	2025
Cases with a single victim losing over ₹50 lakh, Delhi	376	2025
Cybercrime cases registered in Delhi (NCRB)	407 → 404	2023 → 2024
Investment-scam cases in Bengaluru, Delhi-NCR and Hyderabad combined	≈ 65% of cases in major cities	six months to Oct 2025
Potential loss prevented by Delhi Police in five digital arrest cases (four victims aged 65–80)	₹1.53 crore	Oct 2026

The contrast between roughly ₹1,000 crore lost and about 400 registered cybercrime cases a year is the clearest sign of how little of the problem reaches the formal record in Delhi.

5.2 Primary data (to be completed after fieldwork)

> ***DUMMY DATA.*** *Every figure in Section 5.2 comes from a simulated dataset of 412 respondents, generated in Python to show how the results will be reported and tested.*[27] *The tests were run on the simulated data, so the numbers are internally consistent, but they describe no real student. Replace them with fieldwork results.*

Reliability (dummy): awareness scale α = .90; trust in police α = .81; fear of stigma α = .81; legal-literacy test KR-20 = .77. Overall reporting intention: 210 of 412 (51.0%).

Table 2. Profile of respondents (n = 412) [DUMMY DATA]

Variable	Category	n	%
Gender	Female	220	53.4
	Male	188	45.6
	Other	4	1.0
Discipline	Law	113	27.4
	Non-law	299	72.6

ISSN: 2582-6433

Variable	Category	n	%
Level	UG	260	63.1
	PG	124	30.1
	PhD	28	6.8
University type	Public	199	48.3
	Private	213	51.7
Region	Delhi	173	42.0
	Noida / Greater Noida	81	19.7
	Gurugram	74	18.0
	Faridabad	45	10.9
	Ghaziabad	39	9.5
Residence	Family home	175	42.5
	Hostel	146	35.4
	PG accommodation	91	22.1
Total		**412**	**100**

Table 3. Legal literacy: share answering correctly [DUMMY DATA]

Item	Correct answer	Law % (n = 113)	Non-law % (n = 299)	Total %
C1. Police can arrest a person over a video call	False	76.1	56.5	61.9
C2. An arrested person must be produced before a magistrate within 24 hours	True	69.9	54.8	59.0
C3. CBI/ED may ask you to transfer money to a "verification account"	False	86.7	70.6	75.0
C4. An FIR can be filed at any police station (Zero FIR)	True	59.3	39.8	45.1
C5. 1930 is the national cyber-fraud helpline	True	89.4	77.3	80.6
C6. Courts send arrest warrants on WhatsApp	False	81.4	63.9	68.7
C7. Impersonating a public servant is an	True	77.9	59.5	64.6

ISSN: 2582-6433

Item	Correct answer	Law % (n = 113)	Non-law % (n = 299)	Total %
offence under the BNS				
C8. You must stay on camera and not tell anyone during an investigation	False	79.6	57.2	63.3
C9. A complaint can be filed online at cybercrime.gov.in	True	89.4	70.9	76.0
C10. Reporting within hours improves the chance of freezing the money	True	84.1	64.2	69.7
Mean score (out of 10)		**7.94**	**6.15**	**6.64 (SD 2.65)**

Table 4. Exposure and response [DUMMY DATA]

Indicator	Base	n	%
Received a call/message matching the script	All (412)	154	37.4
Joined a video call with the caller	Targeted (154)	41	26.6
Shared personal or bank details	Targeted (154)	14	9.1
Lost money	Targeted (154)	3	1.9
Told family or friends	Targeted (154)	75	48.7
Reported to 1930 / NCRP	Targeted (154)	30	19.5
Filed a police complaint / FIR	Targeted (154)	7	4.5
Reported to university authorities	Targeted (154)	5	3.2

Table 5. Barriers to reporting (ranked by mean, 1 = strongly disagree, 5 = strongly agree) [DUMMY DATA]

Rank	Barrier	Mean	SD
1	"No money was lost, so there was nothing to report"	3.85	0.99
2	"The process takes too long"	3.48	1.04
3	"I did not know where to report"	3.46	1.02
4	"Police would not act"	3.27	1.05
5	"I was unsure which state's police to approach"	3.08	1.06
6	"I felt ashamed / foolish"	2.92	1.07

ISSN: 2582-6433

Rank	Barrier	Mean	SD
7	"My parents would find out"	2.88	1.05
8	"It could hurt my career / visa"	2.73	1.11

Table 6. Binary logistic regression: predictors of reporting intention (n = 412) [DUMMY DATA]

Predictor	B	SE	Wald	Exp(B)	95% CI	p
Awareness score (1–5)	0.109	0.156	0.48	1.11	0.82–1.51	.487
Legal literacy score (0–10)	0.445	0.056	64.01	1.56	1.40–1.74	< .001
Trust in police response (1–5)	0.494	0.145	11.62	1.64	1.23–2.18	.001
Fear of stigma (1–5)	−0.733	0.151	23.50	0.48	0.36–0.65	< .001
Discipline (law = 1)	0.195	0.278	0.49	1.21	0.70–2.09	.484
Gender (female = 1)	0.080	0.239	0.11	1.08	0.68–1.73	.736
Residence (hostel/PG = 1)	0.077	0.241	0.10	1.08	0.67–1.73	.750
Constant	−2.600	0.849	9.38	0.07		.002

Model $\chi^2(7) = 135.78$, $p < .001$; Nagelkerke $R^2 = .374$; Hosmer–Lemeshow $\chi^2(8) = 9.83$, $p = .277$ (adequate fit); correctly classified = 73.5%; highest VIF = 1.16 (no multicollinearity).

Table 7. Summary of hypothesis testing [DUMMY DATA]

Hypothesis	Test	Statistic	Result
H1 Awareness differs by discipline	χ^2 (heard the term); t-test (awareness score)	$\chi^2(1) = 2.30$, $p = .129$; $t(410) = 4.80$, $p < .001$ (law 3.71 vs non-law 3.30)	Partly supported
H2 Legal literacy differs by gender, level, university type	t-test; one-way ANOVA; t-test	Gender $t(406) = -1.66$, $p = .098$; level $F(2, 409) = 4.73$, $p = .009$ (UG 6.34, PG 7.07, PhD 7.46); university $t(410) = -0.52$, $p = .602$	Partly supported (level only)
H3 Legal literacy predicts reporting	Logistic regression	OR = 1.56, p < .001	Supported
H4 Trust in police predicts reporting	Logistic regression	OR = 1.64, p = .001	Supported
H5 Fear of stigma	Logistic	OR = 0.48, p < .001	Supported

ISSN: 2582-6433

Hypothesis	Test	Statistic	Result
reduces reporting	regression		

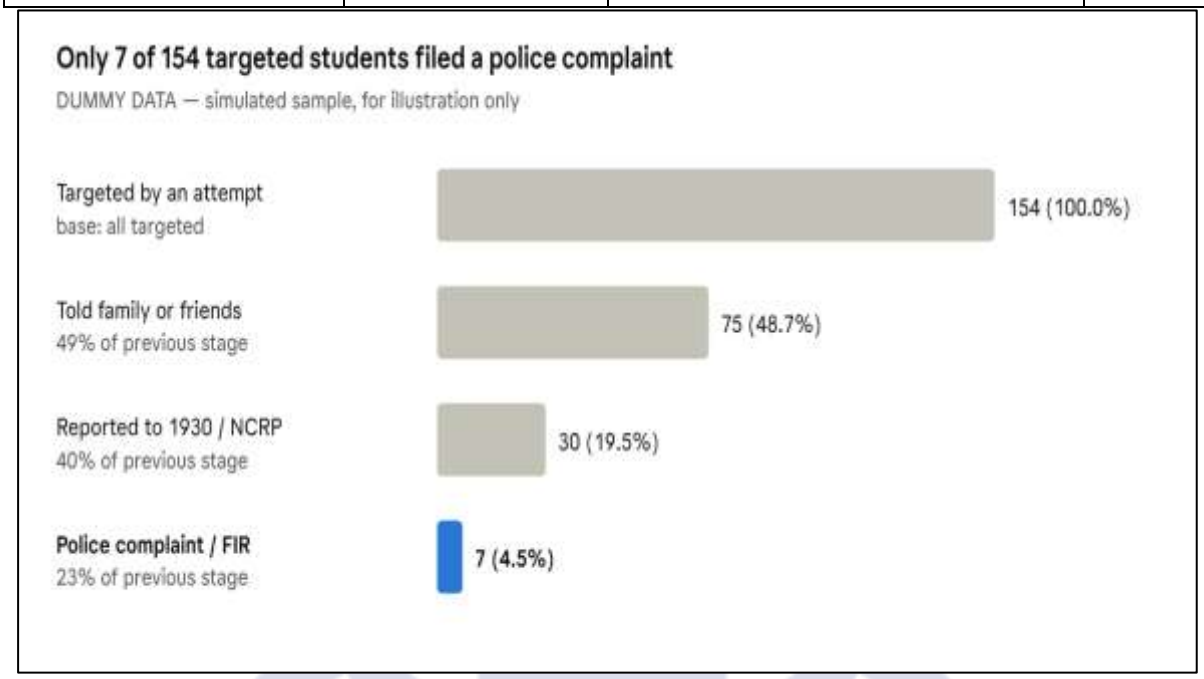

Figure 6 · DUMMY DATA · simulated respondents targeted by a digital arrest attempt (n = 154)

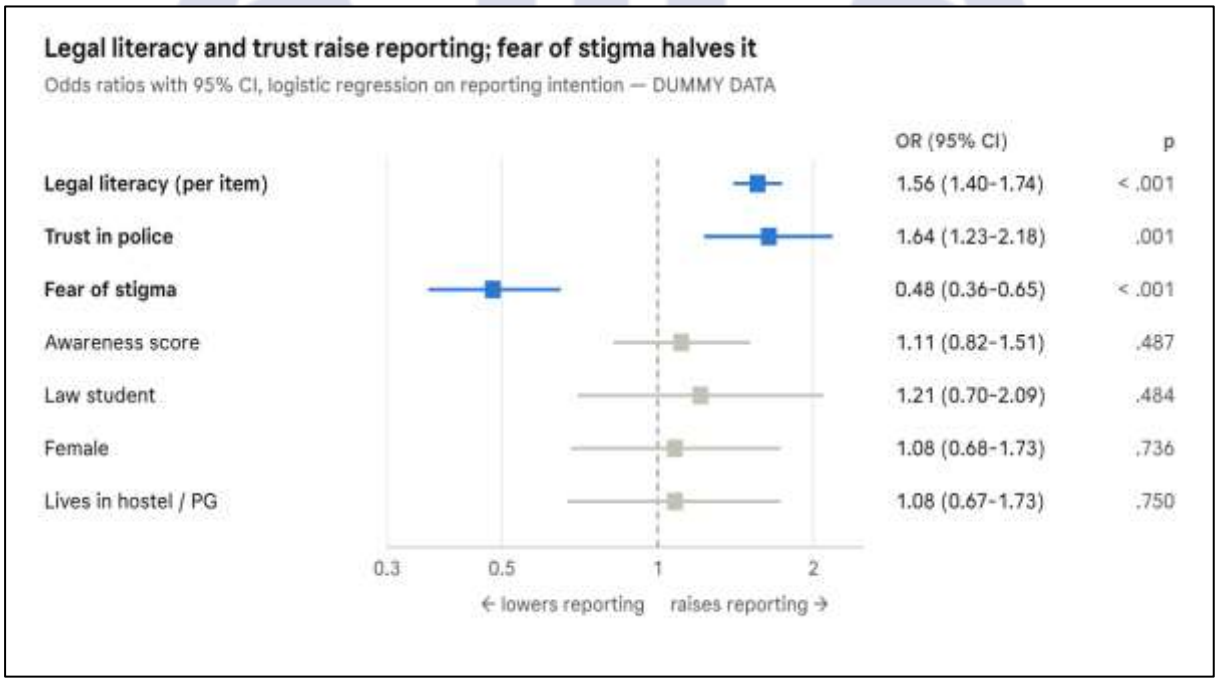

Figure 7 · DUMMY DATA · odds ratios from Table 6, log scale; blue = 95% CI excludes 1

ISSN: 2582-6433

6. Discussion

*Section 6.1 interprets the **dummy data** in Section 5.2 and must be rewritten once real data are in. Sections 6.2–6.4 are argued from law and real secondary data.*

6.1 Interpreting the survey findings

Awareness is high but shallow [DUMMY DATA]. Four in five respondents had heard the term, yet only 61.9% knew that no agency arrests by video call, and only 45.1% knew that a Zero FIR can be filed at any police station. Law students scored higher on both awareness (3.71 vs 3.30) and legal literacy (7.94 vs 6.15 out of 10), but were not significantly more likely to have heard the term. Recognising the label is not the same as knowing the law.

The reporting funnel narrows sharply [DUMMY DATA]. Of 154 targeted students, about half told someone, one in five reported to 1930/NCRP, and fewer than one in twenty filed a police complaint. The top barrier was "no money was lost", which matches the point in Section 6.2 that attempts are not seen as reportable. In the regression, legal literacy (OR 1.56 per correct item) and trust in police (OR 1.64) raised reporting intention, while fear of stigma roughly halved it (OR 0.48). Awareness had no independent effect once legal literacy was in the model. This supports the paper's central claim: knowing the law, not merely knowing the scam, drives reporting.

6.2 Why the law under-counts the problem

Three features of the legal framework push incidents out of the record.

1. **Attempts are invisible.** Most student encounters are likely to end before money moves. An attempted cheating or extortion is an offence, but neither the victim nor the system treats it as reportable. NCRP and FIR data thus measure only *completed* frauds, and policy is built on that partial picture.
2. **Charging practice blurs the crime.** Recording digital arrest as cheating (BNS s. 318) rather than extortion (s. 308) and impersonation (s. 204) hides the coercive core of the offence, and NCRB does not track digital arrest as a separate head. A distinct statistical code — even without a new offence — would allow the problem to be measured.
3. **Jurisdiction confuses victims in NCR.** A student in a Noida hostel, with a bank branch in Delhi and a caller in another country, may not know where to go. BNSS s. 173 answers this with Zero FIR and e-FIR, but the remedy works only if victims know it exists and police stations honour it.

ISSN: 2582-6433

6.3 The liability question

RBI's customer-protection framework limits liability for *unauthorised* transactions. In a digital arrest the victim usually authorises the transfer, but under coercion. Whether consent obtained by impersonating the State is "authorisation" is an open question. A clear RBI position — treating coerced transfers to newly-created or mule accounts as a distinct category — would strengthen the case for reporting quickly, because reporting would then carry a tangible benefit.

6.4 Recommendations

Actor	Measure	Legal / institutional hook
Universities	Make a 30-minute module on arrest rights and cyber fraud part of orientation; name a cyber-safety nodal officer; display 1930 and cybercrime.gov.in on campus	UGC guidance; university codes of conduct
Law faculties and legal aid clinics	Run peer-led "know your arrest rights" sessions and a help-desk for reporting	Legal Services Authorities Act, 1987; clinical legal education[29]
Police (Delhi, UP, Haryana)	Enforce Zero FIR and e-FIR for digital arrest complaints; record attempts as well as losses; publish NCR-wide data	BNSS s. 173
NCRB and I4C	Create a separate head for digital arrest; break data down by age band, including 18–25	Statistical reform, no new offence needed
RBI and banks	Clarify liability for coerced authorised transfers; flag large transfers by young account holders to new payees	RBI customer-liability framework; Supreme Court's direction on AI-based mule detection
Parliament	Consider an aggravated form of s. 204/308 where a public office or court order is impersonated to extort	BNS amendment
Telecom and platforms	Label international calls spoofing Indian numbers; act quickly on reports of impersonation accounts	Sanchar Saathi; IT Rules, 2021[28]

ISSN: 2582-6433

7. Limitations, Future Research and Conclusion

7.1 Limitations

1. **Self-report bias.** Victims may under-state losses or over-state reporting out of embarrassment or social desirability.
2. **Cross-sectional design.** Associations, not causation; the direction between legal literacy and reporting cannot be fixed.
3. **Sampling.** Institutions are chosen purposively within clusters, so results generalise to NCR universities with caution, and not to students in other regions.
4. **Intention vs behaviour.** Reporting *intention* (DV1) may overstate what students would actually do under pressure on a live call.
5. **Secondary data.** I4C figures count complaints, not verified incidents, and published 2025 figures conflict.

7.2 Future research

1. A pre-test/post-test experiment measuring whether a short legal-literacy module raises recognition and reporting.
2. Comparison of students with senior citizens on the same instrument.
3. Analysis of FIRs and charge-sheets to see which BNS sections police actually invoke, and with what outcome.
4. A study of the CBI-led investigation after the Supreme Court's December 2025 direction.

7.3 Conclusion

The digital arrest scam succeeds by imitating legal process, so the first defence is knowledge of legal process. India has the offences (BNS ss. 204, 308, 318–319; IT Act s. 66D), the procedure (BNSS ss. 47, 48, 58, 173) and the reporting channels (1930, NCRP). What it lacks is evidence on whether young people know and use them. This study supplies that evidence for Delhi NCR's university students. **[DUMMY DATA] In the simulated data, each additional correct answer on the legal-literacy test raised the odds of intending to report by about 56%, while fear of stigma roughly halved them.** Closing the gap between awareness and reporting — by teaching arrest rights, honouring Zero FIR and making reporting worthwhile — should sit beside the Supreme Court's enforcement push.

ISSN: 2582-6433

Footnotes

1. I4C figures tabled by the Minister of State for Home Affairs in Parliament in March 2025: 1,23,672 complaints and ₹1,935.51 crore lost in 2024 (Moneylife). ThePrint, citing later MHA data, gives ₹1,918 crore for the same year (ThePrint); the gap probably reflects data revisions.
2. *In Re: Victims of Digital Arrest Related to Forged Documents*, SMWP (Crl.) No. 3 of 2025, order of 1 December 2025, Surya Kant CJI and Joymalya Bagchi J. (Indian Kanoon). The Court asked States to give consent for CBI investigation (LiveLaw); such consent is required under s. 6 of the Delhi Special Police Establishment Act, 1946.
3. NCRB, *Crime in India 2024*: 73,987 of 1,01,928 cybercrime cases had fraud as the motive (The Wire). NCRB counts registered cases (FIRs), not portal complaints, so its totals are far smaller than NCRP's.
4. BNSS ss. 35, 47, 48, 58; Constitution of India, Art. 22(1)–(2). The arrest safeguards laid down in *D.K. Basu v. State of West Bengal*, (1997) 1 SCC 416 — an arrest memo attested by a witness, information to a relative, medical examination — all presuppose physical custody.
5. Mumbai Police case reported by PTI. The student was first called by persons claiming to be from TRAI, then by a "police officer" on WhatsApp video (Business Standard). Cited as a student case although outside NCR.
6. Delhi Police (IFSO) data: residents lost about ₹1,100 crore in 2024 and close to ₹1,000 crore in 2025; at least 376 cases in 2025 involved a single victim losing more than ₹50 lakh (CyberPeace).
7. AISHE 2021–22 (provisional), as reported by Kashmir Life. Verify against the state tables of the AISHE 2021–22 report and update to the latest AISHE round.
8. NCAER analysis of unit-level data from the NSS 79th round Comprehensive Annual Modular Survey, 2022–23 (NCAER). The same survey shows nearly 97% of Indians aged 15–24 own a mobile phone (Digit).
9. YouGov online survey of 1,022 respondents (Telangana Today). A non-probability panel; treat as indicative only.
10. Delhi Police, West District (The Tribune). The accused had opened accounts in several banks for commission-based fraud operations.

ISSN: 2582-6433

11. Ratio computed by the author from Moneylife's figures. The Government's reply to Parliament gives 24,02,579 *financial-fraud* complaints on NCRP in 2025 (Dynamite News); with that denominator the ratio is about 2.3 FIRs per 100 complaints.

12. NCRB does not track digital arrest as a separate category, so all digital-arrest statistics come from I4C's NCRP data (Digital Arrest Scams Explained, 2026).

13. Extortion under BNS s. 308(1) requires that the victim be intentionally put in fear of "injury" and so induced to deliver property. "Injury" under BNS s. 2(14) covers harm to body, mind, reputation or property — wide enough to include fear of arrest and public disgrace.

14. BNSS s. 173(1): information about a cognizable offence may be given orally or by electronic communication, irrespective of the area where the offence was committed.

15. Information given electronically is taken on record once the informant signs it within three days.

16. RBI, *Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions*, DBR.No.Leg.BC.78/09.07.005/2017-18, 6 July 2017. Zero liability applies where a third-party breach is reported within three working days.

17. The loss is reported as ₹1.05 crore (The Leaflet) and as ₹1.5 crore (Moneylife / Bar & Bench). Cite the figure from the Court's own order.

18. Based on searches of open web sources up to November 2026. Before submission, search Scopus, Web of Science, SCC Online, Manupatra and Shodhganga.

19. A finite-population correction is unnecessary: Delhi alone has over 11 lakh students in higher education (note 7), so the sample is far below 5% of the population.

20. W. G. Cochran, *Sampling Techniques* (3rd edn, Wiley 1977). p = 0.5 is used because it gives the largest (most conservative) sample size when the true proportion is unknown.

21. J. C. Nunnally, *Psychometric Theory* (2nd edn, McGraw-Hill 1978), source of the conventional 0.70 threshold. For dichotomous items, G. F. Kuder and M. W. Richardson, "The theory of the estimation of test reliability" (1937) 2(3) *Psychometrika* 151.

22. D. W. Hosmer, S. Lemeshow and R. X. Sturdivant, *Applied Logistic Regression* (3rd edn, Wiley 2013); N. J. D. Nagelkerke, "A note on a general definition of the coefficient of determination" (1991) 78(3) *Biometrika* 691.

ISSN: 2582-6433

23. Indian Council of Medical Research, *National Ethical Guidelines for Biomedical and Health Research Involving Human Participants* (2017), commonly followed by Indian institutional ethics committees for research with human participants.

24. Gurugram figures cover all cybercrime complaints, not only fraud: 19,725 complaints and 597 FIRs in roughly January–early July 2024 (The Tribune, 12 July 2024); 3,557 complaints and 140 FIRs in November 2025 (The420.in).

25. Reply of the Minister of State for Home Affairs to Unstarred Question No. 1341 (Dynamite News). The 2025 loss figure may rise as late complaints are added. Ratios in Figure 5 computed by the author.

26. CFCFRMS, Suspect Registry, SIM and IMEI figures to December 2025: News Karnataka and Free Press Journal. Figure to June 2026: Outlook Money. WhatsApp and Skype blocking: Inc42. I4C also traced 45% of the frauds in its analysis to Cambodia, Myanmar and Laos (Business Standard).

27. Enrolment: note 7. Delhi losses and cases above ₹50 lakh: note 6. Funds held: Devdiscourse / PTI. NCRB Delhi cases: note 3. Investment scams: I4C analysis reported by Business Today. Prevented loss: ThePrint / PTI, 18 Oct 2026.

28. Dummy data method. 412 respondents were simulated in Python with a fixed random seed (2026). Demographic shares were set to plausible values; latent traits generated the Likert and true/false items; reporting intention was drawn from a logistic model whose effect sizes the author chose. Statistics were then computed with SciPy and statsmodels. Because the effects were built in, the "results" demonstrate the analysis — they do not test the hypotheses and must not be cited as findings.

29. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 3 (due diligence by intermediaries). Sanchar Saathi is the Department of Telecommunications portal (sancharsaathi.gov.in); its Chakshu facility takes reports of suspected fraud calls and messages.

30. Legal Services Authorities Act, 1987 (statutory basis for legal aid and legal-literacy work); Bar Council of India Rules of Legal Education, 2008, which make clinical courses part of the LL.B. curriculum.

ISSN: 2582-6433

REFERENCES

Statutes and cases

1. *Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023), ss. 111, 204, 205, 308, 318, 319, 336, 340, 351.*
2. *Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023), ss. 35, 47, 48, 58, 173.*
3. *Information Technology Act, 2000, ss. 66C, 66D.*
4. *Digital Personal Data Protection Act, 2023.*
5. *Constitution of India, Articles 21, 22.*
6. *In Re: Victims of Digital Arrest Related to Forged Documents, Suo Motu Writ Petition (Crl.) No. 3 of 2025, Supreme Court of India, orders dated 17 October 2025 and 1 December 2025. Order of 17 Oct 2025; record of proceedings.*

Books and articles

7. *Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101.*
8. *Button, M., Lewis, C., & Tapley, J. (2009). Fraud typologies and the victims of fraud: Literature review. National Fraud Authority (UK).*
9. *Cialdini, R. B. (1984). Influence: The psychology of persuasion. William Morrow.*
10. *Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review, 44(4), 588–608.*
11. *Cross, C. (2018). (Mis)Understanding the impact of online fraud: Implications for victim assistance schemes. Victims & Offenders, 13(6), 757–776.*
12. *Cross, C., Richards, K., & Smith, R. G. (2016). The reporting experiences and support needs of victims of online fraud (Trends & Issues in Crime and Criminal Justice No. 518). Australian Institute of Criminology.*
13. *Holt, T. J., & Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. Deviant Behavior, 30(1), 1–25.*
14. *Ibrahim, J. M. (2026). Synthesizing "digital arrest" into a standalone offence and the gaps in Indian law under the Bharatiya Nyaya Sanhita, 2023. International Journal of Law Management & Humanities. Link*
15. *Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. Deviant Behavior, 37(3), 263–280.*
16. *Modic, D., & Lea, S. E. G. (2013). Scam compliance and the psychology of persuasion. SSRN Working Paper.*

ISSN: 2582-6433

17. *Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1), 93–114.*
18. *Singh, S. (2025). Digital arrest: The modern-day cyber scam. NITI Aayog. Link*
19. *van de Weijer, S. G. A., Leukfeldt, R., & Bernasco, W. (2019). Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. European Journal of Criminology, 16(4), 486–508.*

Reports, news and commentary (accessed November 2026)

20. *The Legal Shadow of Digital Arrests: Analysing Procedural Loopholes in the BNS and IT Act — LiveLaw.*
21. *Digital Arrest: The Modern-Day Cyber Scam — Drishti Judiciary, March 2026.*
22. *Understanding cyber frauds, digital arrests and how to protect yourself — SCC Online Blog.*
23. *After 465% spike in 2024, MHA data shows digital arrest scams are on a decline — ThePrint, 18 February 2026.*
24. *Digital arrest scam: Govt blocks 83,000 WhatsApp accounts — Odisha Bytes (MHA figures tabled in Parliament, March 2025).*
25. *Closing in on digital arrest scams — Deccan Herald.*
26. *Fraud Alert: India is losing over ₹22,000 crore a year in cyber scams — Moneylife.*
27. *Crime rate fell 6% in 2024; NCRB attributes dip to change from IPC to BNS — The Wire.*
28. *Crime in India 2023: NCRB report highlights surge in cybercrime — summary of NCRB series 2018–2023.*
29. *Lost ₹50 lakh or more to online fraud? Delhi Police has a unit built for exactly that — CyberPeace.*
30. *Digital arrest scam: IIT Bombay student loses Rs 7.29 lakh — Business Standard, November 2024.*
31. *Supreme Court directs CBI to investigate digital arrest scam cases — LiveLaw, 1 December 2025.*
32. *SC orders pan-India CBI probe, asks RBI about AI — Free Press Journal.*
33. *They lost crores. Then came the silence — The Quint.*