Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Enforcement Impediments in Prosecuting Digital Identity Theft in India

Soumya Sahoo

soumyasahooniki@gmail.com

Siksha O Anusandhan University

Om prasada Tripathy

Siksha O Anusandhan University

Research Article

Keywords: digital identity theft, Section 66C, criminal justice attrition, digital evidence, cyber crime enforcement

Posted Date: November 4th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11410413/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License

Additional Declarations: No competing interests reported.

Abstract

India saw 101,928 cybercrime cases filed in 2024. Data on identity theft cases filed with an FIR and prosecuted or otherwise resolved are scarce. This paper uses agency data and a survey of practitioners to examine patterns of identity theft case resolution. According to NCRB data, identity theft cases are often filed alongside cheating cases and recorded under that more serious offense. Trends in cybercrime motivated by fraud, which includes most identity theft cases, are examined nationally. Data on Section 66C of the Information Technology Act, 2000, are examined for 19 major cities. Higher State filing rates were correlated with lower arrest rates. A survey of 220 investigating officers and 80 public prosecutors found that higher agency preparedness increased the case outcomes that officers expected in identity theft cases, while digital-evidence and structural impediments reduced them. These relationships were confirmed using a latent-variable model. Perceived seriousness and own-agency responsibility were not related to expected case outcomes. Readiness for the Bharatiya Nyaya Sanhita, 2023, was mixed. Lack of agency capacity, rather than legal barriers, appears to be the main barrier to resolving identity theft cases.

1. Introduction

India's digital economy relies on digital identity. UPI accounts and Aadhaar-based KYC information, along with one-time passwords and social media accounts, are among the data that can be fraudulently obtained. Stolen identities can quickly be monetized. Reported cyber crimes increased from 9,622 cases in 2014 to 101,928 cases in 2024. Fraud is now the primary purpose of cyber crime in India (MHA 2025b; NCRB 2026). India has implemented two levels of legal protections. Section 66C of the Information Technology (IT) Act, 2000 prohibits identity theft, and Section 66D prohibits cheating by personation using a computer resource (IT Act 2000). On 1 July 2024, the Bharatiya Nyaya Sanhita (BNS), 2023, came into effect alongside the IT Act. The BNS replaced the Indian Penal Code (IPC) and introduced new provisions to combat organized crime (BNS 2023).

Criminalization is just one piece of the puzzle. Other steps in the investigation and prosecution process include filing charges and reaching a verdict. Many identity theft cases are dropped or otherwise fail to move forward at various points. Globally, relatively few reported cybercrimes are investigated or prosecuted (Khan 2024). Law enforcement officials cite a lack of resources and forensic expertise to investigate cybercrimes (Davis 2012; Harkin et al. 2018). India offers an ideal setting for research on identity theft attrition. NCRB data on crime outcomes in India's courts and police forces include information on identity theft but are not widely used in research on identity theft. Few studies have sought the opinions of law enforcement and prosecution officials involved in identity theft cases. This study fills these gaps.

1.1. Legal Framework for Digital Identity Theft

Section 66C of the IT Act 2000 criminalizes misuse of another person's electronic signature, password, or other unique identifier. Section 66D criminalizes cheating by personation using a communication device or computer resource. Offenses under both sections are punishable by a maximum of three years' imprisonment and a fine of up to one lakh rupees. Law enforcement often charges additional offenses of

cheating and forgery along with these IT Act offenses, which are bailable and carry relatively minor penalties. Reforms that took effect in 2024 renumbered cheating and forgery offenses and added new offenses related to organized crime. Other reforms updated laws related to electronic FIRs and searches and other electronic evidence. Table 1 identifies relevant provisions and their uses in law enforcement.

Table 1
Statutory provisions relevant to identity-theft enforcement before and after 1 July 2024.

Element	Before 1 July 2024	From 1 July 2024	Relevance to enforcement
Identity theft; personation using a computer resource	IT Act Sec 66C, 66D	IT Act Sec 66C, 66D (unchanged)	NCRB crime heads 2.3 and 2.4
Cheating by personation	IPC Sec 419	BNS Sec 319(2)	Usually co-charged with Sec 66D
Cheating and inducing delivery of property	IPC Sec 420	BNS Sec 318(4)	Principal charge in financial identity fraud
Forgery; use of forged documents	IPC Sec 465, 468, 471	BNS Sec 336, 340	Misuse of Aadhaar, PAN and KYC documents
Organised crime; petty organised crime	No general provision	BNS Sec 111, 112	Reaches organised cyber-fraud networks
FIR registration and search	CrPC Sec 154, 165	BNSS Sec 173 (e-FIR), Sec 105 (recorded search)	Alters registration and seizure practice
Admissibility of electronic records	Evidence Act Sec 65B certificate	BSA Sec 63 certificate	Certificate defects can defeat prosecution

Sources: IT Act (2000); BNS (2023); BNSS (2023). CrPC = Code of Criminal Procedure, 1973; BNSS = Bharatiya Nagarik Suraksha Sanhita, 2023; BSA = Bharatiya Sakshya Adhiniyam, 2023.

Official practices in recording crime events affect study results. The NCRB reports FIRs filed for each most serious offense committed. An FIR filed under Section 66C for cheating will be classified and reported as a cheating offense. Incidents reported under Section 66C are likely to be a subset of identity theft events. Crime driven by fraud, including incidents reported under Section 66C and cheating, is likely to be a superset of identity theft events (Levi 2017; Correia 2022).

1.2. Literature Review

Research on cybercrime prosecution includes three streams of literature. One stream examines attrition challenges. Cybercriminals act across borders, and key evidence is in the hands of private-sector organizations. These factors create challenges at all stages of the criminal justice process (Holt 2018, 2023; Lusthaus 2024; Nikkhah et al. 2026). Hong and Neilson (2020) find that enhanced punishments do not effectively reduce crime when convictions are rare. Similar findings exist for identity-related crimes in Brazil (Vaz et al. 2026). Other research in Vietnam, Indonesia, and Colombia finds that passing new laws

does not address evidence and attribution challenges (Nguyen et al. 2022; Suseno et al. 2025; Castañeda-Acosta 2025).

The second stream covers police capacity and attitudes. Davis (2012) reported insufficient police resources at the local level to address cybercrime. American and British officers generally believe that cybercrime is best handled by specialist units (Bossler and Holt 2012; Holt and Bossler 2012; Lee et al. 2021). Issues faced by specialist units include high case loads, staff turnover, interjurisdictional problems, and lack of cooperation from private industry (Harkin et al. 2018). Studies have noted a trend away from prosecution toward strategies to reduce harms associated with cybercrime (Whelan et al. 2026; Heeler 2026; Khan 2024). Research has also recommended evidence-based policing approaches for cybercrime (Koziarski and Lee 2020). Cybercrime victims generally do not believe that officers can successfully apprehend cybercriminals (Graham et al. 2020).

The third stream concerns digital evidence. Poor authentication and certification of electronic materials reduce their admissibility in court (Rakha 2024). Bardhan and Ghosh (2026) suggest seven guidelines for assessing the reliability of electronic materials for use in India: authenticity, chain of custody, source reliability, technical competence, other legal admissibility factors, and resistance to tampering. Card fraud and other bank crimes cannot be investigated effectively without competent bank personnel to help analyze bank documents (Shetty and Murthy 2023; Roy and Prabhakaran 2023).

Indian research on identity theft is largely theoretical. Gaps in the Indian IT Act related to AI-based fraud and child exploitation are discussed (Jan and Bashir 2025; Kakkar and Nandrajog 2025; Mhavan and Singh 2025). Other Indian sources discuss the structure and history of the enforcement system (Kethineni 2020; Kshetri 2016). Suggested reforms include protections for ethical hackers and the use of machine learning to study court decisions (Rai et al. 2026; Verma et al. 2026). Limited empirical research on identity theft in India includes studies of victims (Paramasivan et al. 2026; Rawandale et al. 2018), the volume of complaints (Paramasivan et al. 2025), criminal networks in Jamtara and Mewat (Sarkar et al. 2026; Kumar and Verma 2026), and trends in one state (Deb et al. 2026). Studies outside India use administrative and court records to study enforcement activities (Mayer 2016; Correia 2022; Zhang and Dong 2023). There are no similar studies in India.

This literature has four gaps. Researchers have not created a multiyear FIR-to-conviction dataset on cyber fraud cases in India at the State level using government data sources. Researchers have not compared cases filed under Section 66C of the IT Act with other cybercrimes in police and court records. Researchers have not assessed the challenges identified in legal scholarship as barriers to prosecuting cybercrime among police and prosecutors or related outcomes those officials anticipate. Researchers have not studied police and prosecutors' experiences with implementing the new BNS to replace the IPC. Theoretical gaps include a lack of research examining how various barriers to prosecuting cybercrime relate to case outcomes at different stages of the process. This study uses the criminal justice attrition framework, in which attrition refers to the failure to obtain convictions for reported crimes, to analyze data on cybercrime. In line with institutional theory, this study assumes that barriers to conviction in cybercrime cases are

primarily structural rather than based on police and prosecutorial preferences (Kshetri 2016). This study helps to fill these gaps in the literature.

The study makes three contributions. It provides a multiyear, cross-referenced analysis of FIRs, charge-sheets, trials and convictions for fraud-related cyber crime in India, together with a stage-wise comparison of Section 66C cases with other cyber crime. It links official case-outcome data with practitioner assessments to identify the factors associated with attrition. It also provides early evidence on BNS implementation and uses court workload data to estimate backlog clearance times.

1.3. Research Objectives

The study has five objectives:

1. To examine how many cyber-fraud FIRs progress to conviction in 2018–2023.
2. To compare Section 66C identity-theft cases with other cyber crime cases.
3. To examine whether a higher State case load reduces police investigation output.
4. To identify the main difficulties faced by police and prosecutors and their relationship with expected case outcomes.
5. To examine practitioners' experience of the transition from the IPC to the BNS, 2023.

1.4. Hypotheses

- **H1**: *Very few cyber-fraud FIRs in India reach conviction.*
- **H1a**: *The FIR-to-conviction ratio for cyber fraud did not improve from 2018 to 2023.*
- **H1b**: *Section 66C identity-theft cases perform worse than other cybercrime cases in charge-sheeting, conviction and pendency.*
- **H2**: *A higher case load in a State reduces its charge-sheets and arrests per FIR.*
- **H3**: *Higher agency preparedness increases case-outcome expectancy.*
- **H4**: *More digital-evidence impediments reduce case-outcome expectancy.*
- **H5**: *More structural impediments reduce case-outcome expectancy.*
- **H6**: *Higher perceived seriousness and own-agency responsibility increase case-outcome expectancy.*

2. Materials and Methods

2.1. Research Design

The study used a quantitative design with two data sources collected in sequence. Official crime statistics were analyzed first to measure attrition and its variation across States (H1 and H2). A cross-sectional questionnaire survey of officers and prosecutors was then conducted to test which impediments are related to expected case outcomes (H3–H6) and to describe the transition to the BNS. All survey items were closed and scored, so both parts of the study were analyzed statistically. Findings from both data sources are discussed together in the Discussion.

2.2. Secondary Data

All secondary data are from official publications of the Government of India (MHA 2024, 2025a, 2025b; NCRB 2025, 2026). See Table 2 for more information, including links to these publications. Two parliamentary responses provide the same State-level data series from 2019 to 2022. The data in the two sources are identical for all overlapping cells, and the State figures sum to the national totals. Section 66C and Section 66D data available from the NCRB for 19 cities were used to test hypothesis H1b.

The study deals with two concepts and makes a clear distinction between them. Analysis specific to Section 66C of the Information Technology Act is limited to 19 major cities in India where data on crime heads are available for 2023. A total of 944 (22.1%) of 4,278 cybercrime cases reported in 19 major cities in 2023 were under Sections 66C and 66D of the Act (NCRB 2025). At the national and state levels, cyber-related fraud cases were studied rather than cases under Section 66C of the Act. Cases of identity theft reported under cheating or fraud were included in the broader definition of cyber-related fraud, which makes up more than 70% of all cyber crimes in India (NCRB 2026). Findings related to cyber-related fraud should not be taken as findings specific to Section 66C.

Attrition rates were calculated using NCRB definitions. The charge-sheeting rate is the fraction of cases worked by police that were filed on a charge sheet. The conviction rate is the fraction of trials that resulted in conviction. Pendency is the fraction of cases pending investigation or trial at year end. State crime statistics do not track individual cases; State statistics are reported per 100 FIRs registered in the same year. Court congestion is reported as an estimated backlog-clearance time. This is the number of cases pending trial divided by the trials completed in the year.

Table 2
Sources of secondary data.

Source	Data used	Period	Link
MHA, Lok Sabha Unstarred Question No. 452 (2 December 2025), Annexures I–III	Crime-head-wise cyber crime cases; State-wise cyber-fraud cases registered, charge-sheeted, trials completed, convicted; persons arrested	2019–2023	https://www.mha.gov.in/MHA1/Par2017/pdfs/par2025-pdfs/LS02122025/452.pdf
MHA, Rajya Sabha Unstarred Question No. 233 (27 November 2024), Annexures I–II	Crime-head-wise cyber crime cases; State-wise cyber-fraud cases and persons arrested, charge-sheeted and convicted	2018–2022	https://www.mha.gov.in/MHA1/Par2017/pdfs/par2024-pdfs/RS27112024/233.pdf
MHA, Lok Sabha Unstarred Question No. 438 (2 December 2025), Annexure II	All-India cyber crime cases registered	2014–2023	https://www.mha.gov.in/MHA1/Par2017/pdfs/par2025-pdfs/LS02122025/438.pdf
NCRB, Crime in India 2023, Vol. II, Table 9B.4	Police disposal of cyber crime cases by crime head, 19 metropolitan cities	2023	https://data.opencity.in/dataset/crime-in-india-2023/resource/6cfa3ace-4aab-4557-9637-d1ba2c51aa87
NCRB, Crime in India 2023, Vol. II, Table 9B.6	Court disposal of cyber crime cases by crime head, 19 metropolitan cities	2023	https://data.opencity.in/dataset/crime-in-india-2023/resource/904e790a-b189-4f29-a260-6f1bfc408a8b
NCRB, Crime in India 2024	All-India cyber crime cases registered	2024	https://www.ncrb.gov.in/uploads/files/2CrimeinIndia2024-VolumeII.pdf
PIB, Ministry of Home	Cyber-forensic funding by State	2018–2025	https://www.pib.gov.in/PressReleasePage.aspx?PRID=2198253

Source	Data used	Period	Link
Affairs (3 December 2025)			

All links were accessed on 5 October 2026. The compiled dataset is provided as Supplementary Material.

2.3. Survey Instrument, Sample and Procedure

The population included law enforcement and prosecutors. Law enforcement personnel held positions from Sub-Inspector to Deputy Superintendent of Police. Law enforcement personnel were posted at cyber police stations, district cyber cells, and CID or State cyber wings. Prosecutors handled cybercrime trials. Six states were purposefully selected to cover a wide range of experiences with cybercrime: Maharashtra, Uttar Pradesh, Karnataka, Kerala, Assam, and Telangana. A sample of 300 (220 law enforcement personnel and 80 prosecutors) was obtained. The sample is larger than the recommended minimum of 171 to identify a small or medium effect size ($f^2 = 0.10$) with five independent variables and 0.05 and 0.90 levels of significance and power. Surveys were voluntary and anonymous.

Each construct was based on an existing measure and modified for use with Section 66C/66D offenders. All attitudinal measures used five-point scales. Investigating officers completed all blocks of the survey. Prosecutors completed only those blocks applicable to them (see Table 3). Block C (role of the police), one item in Block B on willingness to take further training, and an optional open-ended item at the end of the questionnaire were collected but are not used in the analyses reported here. Case-outcome expectancy is the respondent's rating of how likely a typical identity-theft FIR is to reach offender identification, arrest, charge-sheet and conviction; it measures a perception, not the actual outcome of the case. Own-agency responsibility refers to the number of six offense types an officer reported as falling under his or her own agency. Own-agency responsibility ranges from 0 to 6.

Table 3
Survey constructs, sources and analytical roles.

Block	Construct	Items	Answered by	Adapted from	Role
A	Agency preparedness (AP)	5	Officers	Davis (2012)	Predictor (H3)
B	Digital-investigation proficiency (DP); training hours; willingness to train	3 + 1 + 1	Officers	Holt and Bossler (2012)	Control; profile; not analyzed
C	Role of the police	5	Officers	Bossler and Holt (2012)	Collected; not analyzed
D	Perceived seriousness (PS); agency attribution (OAR)	6 + 6	All	Lee et al. (2021)	Predictors (H6)
E	Digital-evidence impediments (DE)	7	All	Bardhan and Ghosh (2026)	Predictor (H4)
F	Structural impediments (SI)	6	All	Harkin et al. (2018)	Predictor (H5)
G	Case-outcome expectancy (COE)	4	All	Graham et al. (2020)	Dependent variable
H	Court-stage impediments (CI)	5	All	Verma et al. (2026)	Descriptive
I	BNS transition	5	All	Developed for this study	Descriptive
J	Respondent profile	6	All	—	Profile; controls

All items use five-point scales (1 = strongly disagree or very unlikely; 5 = strongly agree or very likely), except training hours (five ordered categories) and agency attribution (four categories).

2.4. Statistical Analysis

Statistical tests were selected according to the type of data and hypothesis. Statistical tests used with secondary data included the Mann–Kendall test for annual trends and the χ^2 test of homogeneity and Cochran–Armitage test for annual changes in proportions. Differences in cyber crime rates, including Section 66C cyber crime, were tested using the Pearson χ^2 or Fisher's exact test. The relationship between State cyber crime caseload and output was tested using least-squares regression with year and State controls and State-clustered standard errors.

For the survey data, confirmatory factor analysis (CFA) was conducted to assess the measurement model, and the goodness of fit was evaluated using standard benchmarks (Hu and Bentler 1999). Internal consistency was evaluated using Cronbach's α, composite reliability and mean inter-item correlations (Clark and Watson 1995). Convergent and discriminant validity were assessed using the average variance extracted and two commonly used discriminant validity measures: the Fornell–Larcker criterion and the heterotrait-monotrait ratio (Fornell and Larcker 1981; Henseler et al. 2015; Hair et al. 2019). The single-

factor test proposed by Harman was used to assess common method variance (Podsakoff et al. 2003). Hypotheses H3 to H6 share an outcome variable and were tested together in a hierarchical regression analysis in which control variables were included in the first block and variables of primary interest in the second block. The following tests were used to check assumptions: the variance inflation factor, Durbin–Watson test, Breusch–Pagan test, and Shapiro–Wilk test. Because the composite scores include measurement error, a latent-variable structural equation model was also estimated. One-sample t-tests, the Friedman test, and the Mann–Whitney U test were used for descriptive analyses. Python 3.13 and packages including SciPy, statsmodels, pingouin, and semopy (Igolkina and Meshcheryakov 2020) were used for all analyses. The significance level was set at $\alpha = 0.05$.

3. Results

3.1. Attrition in Fraud-Motivated Cyber Crime, 2018–2023 (H1a)

Reported cybercrime increased annually from 27,248 cases in 2018 to 86,420 cases in 2023. The annual rate of increase in reported cybercrime was 26.0% (Mann–Kendall $\tau = 1.000$, $p = 0.009$). Reports of IPC crimes related to identity theft increased at an annual rate of 45.2%. These IPC crimes (fraud, cheating, forgery, and false accounts) accounted for 42.9% of all reported cybercrime in 2023. Crimes under Section 66 of the IT Act, including Sections 66C and 66D, accounted for an additional 40.9% of reported cybercrime. Cybercrimes related to identity theft are the most common and fastest-growing types of cybercrime. All statistics cited below are for cybercrimes motivated by fraud, the category of operational cybercrime defined in Section 2.2.

Figure 1 demonstrates weak law enforcement. From 2019 to 2023, 67,567 cybercrime cases involving fraud were filed. Among these cases, 12,014 were charge-sheeted, 1,115 completed trial, and 420 resulted in conviction, a rate of six convictions per 1,000 cases filed. The largest declines occurred after charge-sheeting, with only 9.3 trials completed per 100 charge-sheets. In 2022, 5,213 people were charge-sheeted and 160 convicted. The 2020 conviction peak included 202 convictions in Telangana.

The trend tests in Table 4 show that there were no increases in any output measures with an increase in volume. FIRs increased over time, while charge-sheet and conviction rates did not increase over time. The percentage of FIRs charge-sheeted declined from 25.2% in 2018 to 13.0% in 2021 and partially rebounded. The Cochran–Armitage test for charge-sheeting shows statistical evidence of a rebound in the two largest years. The percentage of FIRs charge-sheeted did not return to the 2018 level. The conviction rate per FIR dropped sharply, to 0.11% in 2023. The number of arrests per 100 FIRs dropped from 53.0 in 2018 to 18.8 in 2023. H1a is supported for fraud-driven cybercrime.

Table 4
Trend tests on the cyber-fraud attrition funnel, All India, 2018–2023 (H1a).

Trend Tests						
Test	Indicator	Period	Statistic	Z / df	Sig.	Direction
Mann–Kendall	Cases registered (FIR volume)	2018–2023	τ = 1.000	Z = 2.630	.009	increasing
Mann–Kendall	Charge-sheet / FIR ratio (%)	2018–2023	τ = −0.067	Z = 0.000	1.000	no trend
Mann–Kendall	Convictions / FIR (%)	2018–2023	τ = −0.067	Z = 0.000	1.000	no trend
Mann–Kendall	Persons arrested per 100 FIRs	2018–2023	τ = −0.600	Z = −1.503	.133	no trend
Mann–Kendall	Conviction rate (% of trials completed)	2019–2023	τ = −0.200	Z = −0.245	.806	no trend
Pearson χ² (homogeneity)	Charge-sheeted vs not, by year	2018–2023	χ² = 485.958	df = 5	.000	
Cochran–Armitage trend	Charge-sheeted / FIR	2018–2023		Z = 4.486	.000	increasing
Cochran–Armitage trend	Convicted / FIR	2018–2023		Z = −8.042	.000	decreasing

Mann–Kendall tests use six annual observations (five for the conviction rate); the smallest attainable two-sided p for n = 6 is about 0.009.

3.2. Disposal of Section 66C Cases Compared with Other Cyber Crime (H1b)

In 2023, the 19 metropolitan cities had 789 active Section 66C investigations, including 322 new cases. There were also 348 Section 66C cases in trial. Figure 2 shows how Section 66C investigations and cases compare with Section 66D investigations and cases and with all cybercrime investigations and cases. Most active investigations and trials involve other cybercrime cases. At the end of 2023, 72% of Section 66C cases were still being investigated, and over 90% of Section 66C cases referred to trial were unresolved.

The tests in Table 5 indicate that identity theft was not under a particular disadvantage. The charge-sheeting rate for identity theft was the same as the rate for other cybercrime. The backlog rate in investigating identity theft was lower, and the court backlog rate for identity theft was the same as for other cybercrime. The conviction rate for completed identity theft trials was higher but not statistically significant. The conviction rate per identity theft case referred to trial was significantly higher (odds ratio of 2.71). Many of the same factors affect all cybercrime cases. Of 348 Section 66C cases referred to trial, only 16 were resolved in 2023, meaning a backlog that would take 20.6 years to clear. All cyber crime cases combined would take 29.2 years to clear, and Section 66D cases would take 59.4 years. H1b is not supported. H1 is supported: very few cyber-fraud FIRs reach conviction (H1a), but Section 66C cases do not perform worse

than other cyber crime (H1b). In cities where other forms of cybercrime can be separated from identity theft under Section 66C, identity theft seems to face no particular disadvantage relative to other forms of cybercrime.

Table 5
Section 66C identity theft versus all other cyber crime, 19 metropolitan cities, 2023 (H1b).

Crosstabulation Tests							
Disposal outcome	Sec 66C (%)	Other cyber crime (%)	Test	Value	df	Sig. (2-sided)	Odds ratio (66C vs other)
Charge-sheeted vs final report (of cases disposed by police)	51.1	51.9	Pearson χ^2	0.042	1	.837	0.971
Pending investigation at year end (of total for investigation)	72.2	75.6	Pearson χ^2	4.422	1	.035	0.839
Pending trial at year end (of total for trial)	94.5	96.5	Pearson χ^2	3.440	1	.064	0.636
Convicted vs acquitted/discharged (of trials completed)	50.0	26.7	Fisher's exact			.079	2.745
Convicted (of total cases for trial)	2.30	0.86	Fisher's exact			.015	2.712

“Other cyber crime” equals total cyber crime minus Section 66C. Pearson χ^2 without continuity correction; Fisher’s exact test where expected counts are below 5.

3.3. Case Load and Investigative Throughput (H2)

The State panel consists of 89 State-years from 20 States and Union Territories with at least 20 cyber-fraud FIRs. Table 6 shows the relationship between case load and investigative throughput. The relationship between case load and the charge-sheet rate was negative but not statistically significant in the pooled analysis and only marginally significant within States (B = − 5.033, p = 0.061). The relationship between case load and arrests was significantly negative (p = 0.007). A 2.7 times difference in the number of FIRs was associated with 8.3 fewer arrests per 100 FIRs. Rank correlation analyses confirm these findings (ρ = −0.184, p = 0.084 for charge-sheets; ρ = −0.378, p < 0.001 for arrests). H2 is partially supported.

Table 6
Regression of State investigative throughput on case load, 2018–2023 (H2).

Coefficients			
Statistic	Model 1	Model 2	Model 3
Dependent variable	Charge-sheets per 100 FIRs	Charge-sheets per 100 FIRs	Arrests per 100 FIRs
Fixed effects	Year	State and year	Year
ln(FIRs): B	−2.186	−5.033	−8.304
Robust std. error	1.907	2.682	3.100
z	−1.146	−1.877	−2.679
Sig.	.252	.061	.007
95% CI for B	[− 5.924, 1.552]	[− 10.290, 0.224]	[− 14.379, − 2.228]
R^2	0.070	0.642	0.223
Adjusted R^2	0.002	0.500	0.166
N (State-years)	89	89	89

Ordinary least squares with standard errors clustered by State/UT; year and State dummies not shown.

3.4. Respondent Profile

Figure 3 profiles the respondents. Officers made up 73.3% of respondents. Inspectors and Sub-Inspectors were the most common ranks. Most officers worked in cyber police stations or district cyber cells. Respondents represented each state at 13.7% to 21.0% of the sample. The mean length of service was 13.2 years (SD = 6.2), with a mean of 5.0 years of cyber-related experience (SD = 2.8). On average, respondents investigated 17.9 cases involving Section 66C/66D in the last year. Training varied. Twenty-two percent of officers reported receiving eight or fewer hours of cybercrime training over two years.

3.5. Measurement Model

A CFA of the 25 items for the officer sample assessed the five-factor model (Table 7). The CFA results indicated excellent model fit: $\chi^2(265) = 244.11$ ($p = 0.817$), CFI = 1.000, TLI = 1.000, RMSEA = 0.000, and SRMR = 0.050 (Hu and Bentler 1999). Standardized factor loadings were statistically significant ($p < 0.001$) and ranged from 0.47 to 0.68. Composite reliability for all factors except digital-investigation proficiency (0.579) and structural impediments (0.691) was 0.70 or higher.

Table 7
Measurement model: factor loadings, reliability and convergent validity (investigating officers, n = 220).

Measurement Model						
Construct	Item	CFA λ	Cronbach's α	CR	AVE	MIIC
Agency preparedness	A1	0.586	0.700	0.702	0.321	0.318
	A2	0.607				
	A3	0.475				
	A4	0.568				
	A5	0.588				
Digital-investigation proficiency	B1	0.574	0.577	0.579	0.315	0.312
	B3	0.602				
	B4	0.504				
Digital-evidence impediments	E1	0.607	0.768	0.770	0.326	0.322
	E2	0.667				
	E3	0.504				
	E4	0.572				
	E5	0.622				
	E6	0.481				
	E7	0.519				
Structural impediments	F1	0.497	0.686	0.691	0.273	0.268
	F2	0.624				
	F3	0.548				
	F4	0.504				
	F5	0.468				
	F6	0.479				
Case-outcome expectancy	G1	0.544	0.700	0.702	0.372	0.370
	G2	0.558				
	G3	0.683				
	G4	0.644				

CFA λ = standardised loading (all $p < 0.001$). CR = composite reliability; AVE = average variance extracted; MIIC = mean inter-item correlation. CFA fit: $\chi^2(265) = 244.11$, CFI = 1.000, TLI = 1.000, RMSEA = 0.000, SRMR = 0.050.

AVE values were less than the typical threshold of 0.50 for all constructs (0.27–0.37). This is a limitation of the measures. Three facts help to address it. First, the measures assess relatively wide-ranging topics. For instance, the digital-evidence impediments scale covers seven separate evidence criteria. This makes it difficult for the items to be highly related to one another. The mean inter-item correlation for each scale (0.27–0.37) falls within the recommended range of 0.15–0.50 for wide-ranging constructs (Clark and Watson 1995). Second, deleting items with factor loadings below 0.50 did not increase the AVE above 0.37 for any scale. All items were kept to maintain content validity. Third, hypothesis tests using a latent-variable model that adjusts for measurement error are presented in Section 3.6. Digital-investigation proficiency has the lowest reliability of the constructs (α = 0.577) and is included as a control variable only.

Discriminant validity was established (Table 8). The square root of the AVE for each construct (0.52 or higher) was greater than the highest correlation between that construct and any other construct (0.35). Heterotrait-monotrait correlations were all below 0.85 (highest of 0.501) (Fornell and Larcker 1981; Henseler et al. 2015). Skewness and kurtosis of the composites were within ± 2 (Hair et al. 2019). Results of Harman's single-factor test showed that the first factor accounted for 16.54% of the variance, so common method variance is not a concern (Podsakoff et al. 2003).

Table 8
Descriptive statistics, correlations, square root of AVE and heterotrait–monotrait ratios (investigating officers, n = 220).

Correlations							
Construct	Mean	SD	AP	DP	DE	SI	COE
AP	3.30	0.81	.567	.405	.242	.209	.501
DP	3.44	0.87	.253**	.562	.180	.302	.453
DE	3.87	0.72	−.171*	−.115	.571	.149	.339
SI	4.17	0.61	−.130	−.160*	.013	.523	.368
COE	2.63	0.91	.353**	.285**	−.236**	−.255**	.610

Below the diagonal: Pearson correlation; diagonal: √AVE from the CFA; above the diagonal: HTMT ratio. ** $p < 0.01$; * $p < 0.05$ (two-tailed). AP = agency preparedness; DP = digital-investigation proficiency; DE = digital-evidence impediments; SI = structural impediments; COE = case-outcome expectancy.

3.6. Determinants of Case-Outcome Expectancy (H3–H6)

H3–H6 were examined simultaneously using a two-step hierarchical regression (see Table 9). These analyses provide measures of the strength of the relationships between variables, controlling for other variables. The three control variables in Step 1 accounted for 10.0% of the variance in the dependent

variable ($F(3, 216) = 8.031$, $p < 0.001$). The five independent variables entered in Step 2 explained an additional 13.9% of the variance (F change$(5, 211) = 7.681$, $p < 0.001$). The overall R^2 was 0.239. All assumptions for these tests were met. None of the variance inflation factors exceeded 1.14. The Durbin–Watson statistic was 1.89. The Breusch–Pagan test indicated the absence of heteroscedasticity ($p = 0.871$). Residuals were normally distributed (Shapiro–Wilk $p = 0.505$).

Table 9
Hierarchical regression of case-outcome expectancy on enforcement factors (H3–H6; investigating officers, n = 220).

Coefficients									
	Model 1 (controls)		**Model 2 (controls + predictors)**						**Latent SEM**
Predictor	β	t	B	Std. Error	β	t	Sig.	VIF	β
(Constant)		4.971	2.931	0.851		3.444	0.001		
Digital-investigation proficiency	0.280	4.283	0.175	0.067	0.168	2.624	0.009	1.139	0.261*
Years in cyber unit	0.123	1.901	0.031	0.020	0.095	1.533	0.127	1.056	0.119
Sec 66C/66D caseload (12 months)	−0.065	−0.998	−0.008	0.012	−0.041	−0.671	0.503	1.057	−0.062
H3: Agency preparedness			0.283	0.071	0.253	3.976	0.000	1.120	0.318**
H4: Digital-evidence impediments			−0.196	0.080	−0.155	−2.458	0.015	1.101	−0.199*
H5: Structural impediments			−0.280	0.093	−0.189	−3.027	0.003	1.079	−0.202*
H6: Perceived seriousness			0.026	0.113	0.014	0.229	0.819	1.061	0.012
H6: Own-agency responsibility			−0.006	0.048	−0.008	−0.129	0.897	1.040	−0.035

Model 1: $R^2 = 0.100$, adjusted $R^2 = 0.088$, $F(3, 216) = 8.031$, $p < 0.001$. Model 2: $R^2 = 0.239$, adjusted $R^2 = 0.210$, $F(8, 211) = 8.278$, $p < 0.001$; $\Delta R^2 = 0.139$, F change$(5, 211) = 7.681$, $p < 0.001$; Durbin–Watson = 1.890.

Latent SEM: AP, DP, DE, SI and COE modelled as latent variables; $\chi^2(371) = 383.95$, CFI = 0.985, TLI = 0.984, RMSEA = 0.013. *** $p < 0.001$; ** $p < 0.01$; * $p < 0.05$.

Dependent variable: case-outcome expectancy. B = unstandardised coefficient; β = standardised coefficient.

Agency readiness had the strongest positive correlation (β = 0.253, p < 0.001), confirming H3. Digital-evidence barriers were negatively correlated with expectancy (β = −0.155, p = 0.015), confirming H4. Other structural barriers were also negatively correlated (β = −0.189, p = 0.003), confirming H5. Perceived severity (β = 0.014, p = 0.819) and own-agency accountability (β = −0.008, p = 0.897) were not correlated with case-outcome expectancy, rejecting H6. Of the controls, only skills (β = 0.168, p = 0.009) were significantly related to case-outcome expectancy.

Two robustness tests confirm the findings. First, a latent-variable analysis accounting for measurement error was a good fit and yielded the same pattern of results (last column of Table 9). Preparedness (β = 0.318), digital-evidence obstacles (β = −0.199), and structural obstacles (β = −0.202) were significant, but seriousness and responsibility were not. Second, the sample included prosecutor respondents who completed the evidence, structural, and seriousness questions. An analysis using all 300 respondents produced similar results. Digital-evidence and structural obstacles (β = −0.254, p < 0.001) were significant for prosecutors, but seriousness was not (p = 0.290), and there was no difference between prosecutors and police respondents (p = 0.606). The cross-sectional nature of the data limits the conclusions about causality that can be drawn.

3.7. Perceived Impediments and the BNS Transition

All eighteen obstacles received mean scores well above the midpoint on a five-point scale (one-sample t-tests, all p < 0.001); see Fig. 4. Structural obstacles were most highly reported. Three structural obstacles received the highest mean scores: slow delivery of services from banks, telecom companies, and other intermediaries (M = 4.28; 79% agreement), foreign offenders, and high caseloads. Among evidence-related obstacles, certificate admissibility and the reliability of intermediary records were highly reported. Reporting differed significantly among the three types of obstacles (Friedman $\chi^2(2) = 37.99$, p < 0.001). Structural obstacles were most highly reported, compared with other types of obstacles (Wilcoxon tests with Bonferroni adjustment, all p < 0.001). Evidence and other courtroom obstacles were equally reported. Police and prosecutors agreed on all common factors (Mann–Whitney U-tests, all p > 0.05).

Practitioners' expectations decrease as the process unfolds (Fig. 5a). About 36.7% believed the culprit was known. Just 14.7% believed a conviction was likely, and 64.7% believed a conviction was unlikely (Friedman $\chi^2(3) = 89.63$, p < 0.001). Preparedness for the BNS was modest (Fig. 5b). About half of the respondents reported having received training on the BNS (45.7%) and understanding the new provisions (50.7%). Just 20.7% had used new sections on organized crime (111 and 112). About 57.7% reported that the implementation of electronic FIR rules affected their behavior. Just over half (51.7%) reported that charge framing took longer under the BNS.

4. Discussion

The official and survey data reach similar conclusions. Less than 1% of cybercrime FIRs filed for fraud-related crimes result in conviction, and conviction rates have declined over time with increasing filings.

Officers and prosecutors generally report lower expectations of conviction at each stage of the process. Khan (2024) found that data on cybercrime case outcomes are not publicly available in Singapore. This paper provides data on cybercrime case outcomes in India. These outcomes are very low.

The findings suggest that capacity issues are a common problem. Registration of cyber-fraud cases increased nearly sixfold at the national level from 2018 to 2023 (3,353 to 19,466 FIRs) without a similar increase in charge-sheets or convictions. At the state level, higher registration rates were correlated with lower arrest rates on FIRs and perceptions of high case loads as one of the greatest challenges among practitioners. These results are similar to those reported by Harkin et al. (2018) for specialized units in Australia. They also align with institutional theories of India's response to cybercrime, which emphasize formal capacity (Kshetri 2016).

The greatest attrition occurs not at the arrest stage but between the filing of charges and conviction. All types of offenses had more than 94% of cases pending in court, with Section 66C offenses taking about 20 years to work their way through the system. Cases are not being dismissed but are building up in the courts. Verma et al. (2026) have identified delays in processing as one impediment to effective law enforcement. The information presented here provides evidence to support their conclusion. Other research supports the conclusion that sanctions may be ineffective deterrents for certain crimes with low conviction rates (Hong and Neilson 2020; Vaz et al. 2026).

Digital evidence challenges were negatively related to favorable case outcomes, with certificate admissibility identified as the biggest challenge. These findings align with the reliability standards set by Bardhan and Ghosh (2026) and calls for evidence-related reforms (Rakha 2024). Section 66C identity theft cases were not judged less favorably than other types of cybercrime, contrary to previous legal scholarship suggesting that identity theft would be more difficult to prosecute (Jan and Bashir 2025; Kakkar and Nandrajog 2025). Evidence related to third-party records and certificates is relevant to most cybercrimes, not just identity theft.

Structural barriers received the highest ratings and were correlated with lower expectations, even after controlling for other variables. Offenders and intermediaries operating across jurisdictions were reported in Jamtara and Mewat (Sarkar et al. 2026; Kumar and Verma 2026). Preparedness was most strongly correlated with higher expectations, as found by Davis (2012). Self-reported perceptions of the importance and personal responsibility related to cybercrime were not significantly correlated with expectations. Studies in the US and UK have shown that law enforcement officials view cybercrime as the responsibility of specialized units (Bossler and Holt 2012; Lee et al. 2021). Results from this study suggest that personal responsibility for cybercrime without other resources is not correlated with higher expectations. Low expectations among law enforcement officials are consistent with victims' perceptions of law enforcement's lack of resources (Graham et al. 2020).

The BNS transition has similar effects. Changes in registration behavior are evident, but few respondents were familiar with and had completed charges under Sections 111 and 112 of the BNS, and most respondents found charge framing more time-consuming. Similar delays in registration behavior have been observed in Indonesia following adoption of the Criminal Code (Suseno et al. 2025). Adding new crimes to

the law expands practitioners' options but does not provide other benefits needed for effective use of those options.

Several steps can be taken to overcome these problems Establish cyber courts and special divisions of current courts with annual goals to reduce the backlog of cases Provide forms for certifying evidence and require hash certification at the time of seizure Appoint nodal officers to certify evidence obtained from intermediaries to speed up evidence collection Establish deadlines for banks, telecommunication companies, and other service providers to respond to other challenges Funding for these programs should be based on the number of cases Himachal Pradesh received ₹7 29 crore in cyber-forensic assistance for 127 cases in 2023 Telangana received ₹2 98 crore in cyber-forensic assistance for 18,236 cases (PIB 2025) Training should cover crimes under BNS Sections 318(4), 319(2), 336, and 340, as well as Sections 66C and 66D Other steps can be taken to prevent and punish cybercrime (Heeler 2026; Whelan et al 2026)

5. Conclusions

This paper examines reasons for case attrition in digital identity theft cases from FIR to conviction in India. The analysis uses cross-validated government data and a survey of 300 police and prosecutors. National trends in digital identity theft were studied using data on fraud crimes, which capture most identity theft cases reported in government data. Section 66C was studied directly where data on other types of crime are available. Attrition occurs at all stages of the process, particularly between filing of charges and conviction. Lack of resources and other institutional constraints, not legal barriers, play major roles in case attrition.

For Objective 1, 0.62% of FIRs filed for fraud-related cyber crimes in 2019–2023 resulted in a conviction. Rates of conviction for fraud-related cyber crimes decreased over time. For Objective 2, outcomes did not differ for Section 66C cases and other cyber crimes, but cases under Section 66C would take approximately 21 years to process. For Objective 3, higher overall caseloads in States were correlated with lower arrest rates for cybercrime-related FIRs. For Objective 4, the main difficulties reported by police and prosecutors were digital-evidence and structural impediments. Higher agency preparedness increased expected case outcomes, while digital-evidence and structural impediments reduced them. Perceived seriousness and own-agency responsibility did not affect expected case outcomes. For Objective 5, changes to registration practices under the BNS have occurred, but few provisions related to organized crime have been used.

In addition to the Indian evidence presented, this study demonstrates ways to use publicly available data on case disposals and other information about legal practice to identify and investigate case attrition. The study's evidence suggests a theory of attrition based on limited resources and cooperation: higher rates of case attrition in Indian states with fewer resources and less cooperation among courts. This research design could be used in other jurisdictions with available data on stage-wise case disposals.

These findings provide new information. Legal studies of Sections 66C and 66D described potential legal problems but did not include other relevant information, such as outcomes (Jan and Bashir 2025; Kethineni 2020). This study provides information on attrition and highlights the importance of capacity relative to

legal definitions. Verma et al. (2026) identified issues related to lengthy trials and lack of digital evidence but did not evaluate them. This study evaluates those factors. Bardhan and Ghosh (2026) used expert opinion to rank the importance of evidence. This study finds that practitioners similarly rank the importance of evidence. Other studies in India have focused on victims and complaints in individual States (Paramasivan et al. 2025, 2026; Deb et al. 2026). This study offers new information about enforcement activities in six States.

This study's limitations suggest areas for future research Limited time coverage of national data on Section 66C convictions prevents generalization to national trends in Section 66C convictions and comparison beyond 19 cities in 1 year Same-year state data on FIR filings limit longitudinal study of specific cases The types of principal offenses defined by the NCRB do not include all forms of identity theft Measures of capacity at the state level were limited to caseload data A cross-sectional, self-administered survey prevented causal interpretations No data exist on case outcomes, and only six states were included in the national sample AVEs for scales were less than 0 50, but results of a latent variable analysis were consistent with other results

Several directions for future research follow from these limitations. Potential approaches to measurement include using NCRB crime statistics and requests under the Right to Information Act to obtain information on arrests under Sections 66C and 66D across India between 2017 and 2024. Data validation techniques like those described by Correia (2022) can be used in this research. Other strategies include collecting case-level data on arrests, charges, and trial outcomes to obtain other data on Section 66C and 66D cases and compare expected and realized outcomes. The machine-learning analysis of court records suggested by Verma et al. (2026) can be used to study Section 66C and 66D cases and reasons for acquittal, including flaws in complaint certificates. Data like those collected by Mayer (2016) can be used for this purpose. The complaint data of Paramasivan et al. (2025) can be combined with FIR data to study losses that occur before an FIR is filed. Data on State resources, such as the number of cyber police stations and forensic labs (PIB 2025), can also be collected. Finally, the scales can be improved by adding more similar items to increase convergent validity.

Additional research should broaden the topic. Fresh studies of AI- and deepfake-related fraud are needed, as legal scholarship suggests that prosecuting these offenses may be more difficult (Jan and Bashir 2025; Kakkar and Nandrajog 2025). Research is also needed on cross-border fraud rings based in Jamtara and Mewat to explore the implications of cross-border collaboration for case outcomes (Sarkar et al. 2026; Kumar and Verma 2026). Case outcomes under the BNS from 2026 forward should be examined to assess the impact of Sections 111 and 112 of the BNS on prosecution success. A national panel survey could help establish causality. Other measures, such as funds frozen after calls to the 1930 helpline, may help assess program effectiveness (Whelan et al. 2026; Khan 2024).

Combined, these measures may help India build a tool to track current and future identity theft-related losses. Advantages of such a tool for India include improved knowledge about trends in identity theft losses and the impact of public policies on those trends.

Declarations

Author Contribution

Soumya Sahoo, the first author,contributed to the conceptualization, research, data collection, analysis and interpretation of the findings. Om prasada Tripathy , the second author contributed to the preparation of the original manuscript, reviewed relevant literature, and contributed to the development of the research methodology.

Data Availability

I conducted the field study and collected the primary data for the research.

References

1. Bardhan, Ruhit, Rajdeep Ghosh. 2026. Evaluation of Digital Evidence Reliability Using Neutrosophic TOPSIS: An Indian Cyber-Law Perspective. *Boletim da Sociedade Paranaense de Matemática* 44:81451. https://doi.org/10.5269/bspm.81451
2. BNS. 2023. The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023). New Delhi: Government of India. In force from 1 July 2024.
3. BNSS. 2023. *The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023) and The Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023)*. New Delhi: Government of India.
4. Bossler, Adam M., and J. Holt Thomas. 2012. Patrol Officers' Perceived Role in Responding to Cybercrime. Policing: An International Journal of Police Strategies & Management 35: 165–81. https://doi.org/10.1108/13639511211215504
5. Castañeda-Acosta, Ana Lilia. 2025. 35 Cybercriminals: Challenges and Lessons Learned from Impunity in Cyberspace. *Logos Ciencia & Tecnología* 17:50–69. https://doi.org/10.22335/rlct.v17i2.2129
6. Clark, Lee Anna, and David Watson. 1995. Constructing Validity: Basic Issues in Objective Scale Development. *Psychological Assessment* 7:309–319. https://doi.org/10.1037/1040-3590.7.3.309
7. Correia, Sara Giro. 2022. *International Journal of Population Data Science* 7:9. https://doi.org/10.23889/ijpds.v7i1.1721. Making the Most of Cybercrime and Fraud Crime Report Data: A Case Study of UK Action Fraud.
8. Davis, Justin T. 2012. Examining Perceptions of Local Law Enforcement in the Fight against Crimes with a Cyber Component. *Policing: An International Journal of Police Strategies & Management* 35:272–284. https://doi.org/10.1108/13639511211230039
9. Deb, Nirdesh, Sharad Shekhawat, Sanjib Debnath, and Rakhal Das. 2026. An Analysis of Cybercrime Trends in India with a Focus on Tripura (Pre and During COVID-19). *Boletim da Sociedade Paranaense de Matemática* 44:78912. https://doi.org/10.5269/bspm.78912
10. Fornell, Claes, and David F. Larcker. 1981. Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research* 18:39–50.

https://doi.org/10.1177/002224378101800104

11. Graham, Amanda, Teresa C. Kulig, and Francis T. Cullen. 2020. Willingness to Report Crime to the Police: Traditional Crime, Cybercrime, and Procedural Justice. *Policing: An International Journal* 43:1–16. https://doi.org/10.1108/PIJPSM-07-2019-0115
12. Hair, Joseph F., William C. Black, Barry J. Babin, and Rolph E. Anderson. 2019. *Multivariate Data Analysis*. 8th ed. Andover: Cengage Learning.
13. Harkin, Diarmaid, Chad Whelan, Lennon, and Chang. 2018. *Police Practice and Research* 19:519–536. https://doi.org/10.1080/15614263.2018.1507889. The Challenges Facing Specialist Police Cyber-Crime Units: An Empirical Analysis.
14. Heeler, Angela E. 2026. Online Crime as Serious and Organised Crime: A View from Britain's Law Enforcement. *Global Crime* 27:242–272. https://doi.org/10.1080/17440572.2026.2653231
15. Henseler, Jörg, Christian M. Ringle, and Marko Sarstedt. 2015. A New Criterion for Assessing Discriminant Validity in Variance-Based Structural Equation Modeling. *Journal of the Academy of Marketing Science* 43:115–135. https://doi.org/10.1007/s11747-014-0403-8
16. Holt, Thomas J. 2018. Regulating Cybercrime through Law Enforcement and Industry Mechanisms. *The Annals of the American Academy of Political and Social Science* 679:140–157. https://doi.org/10.1177/0002716218783679
17. Holt, Thomas J. 2023. Understanding the State of Criminological Scholarship on Cybercrimes. *Computers in Human Behavior* 139:107493. https://doi.org/10.1016/j.chb.2022.107493
18. Holt, Thomas J., Adam M. Bossler, and Cyberpsychology. 2012. *Behavior and Social Networking* 15: 464–472.
19. Hong, Ye, William Neilson. 2020. Cybercrime and Punishment. *The Journal of Legal Studies* 49:431–466. https://doi.org/10.1086/711715
20. Hu, Li-tze, Peter M. Bentler. 1999. Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria versus New Alternatives. *Structural Equation Modeling* 6:1–55. https://doi.org/10.1080/10705519909540118
21. Igolkina, Anna A., and Georgy Meshcheryakov. 2020. semopy: A Python Package for Structural Equation Modeling. *Structural Equation Modeling* 27:952–963. https://doi.org/10.1080/10705511.2019.1704289
22. IT Act. 2000. *The Information Technology Act, 2000 (Act No. 21 of 2000), as amended by the Information Technology (Amendment) Act, 2008*. New Delhi: Government of India.
23. Jan, Saima, Anna Bashir. 2025. Combating AI-Enabled Identity Theft: Strengthening Legal Frameworks in India. *Journal of Intellectual Property Rights* 30:583–590. https://doi.org/10.56042/jipr.v30i5.15633
24. Kakkar, Leena, and Anju B. Nandrajog. 2025. Managing Legal Challenges in the Current Digital Era: The Deepfake Dilemma in an Indian Context. In *Deepfake Technology Dilemmas: Mastering Managerial Navigation*, 129–148. New York: Nova Science.
25. Kethineni, Sesha. 2020. Cybercrime in India: Laws, Regulations, and Enforcement Mechanisms. In The Palgrave Handbook of International Cybercrime and Cyberdeviance. Edited by Thomas J. Holt and

Adam M. Bossler. Cham: Palgrave Macmillan, pp. 305–26. https://doi.org/10.1007/978-3-319-78440-3_7

26. Khan, Azfer A. 2024. Reconceptualizing Policing for Cybercrime: Perspectives from Singapore. *Laws* 13:44. https://doi.org/10.3390/laws13040044
27. Koziarski, Jacek. 2020. and Jin Ree Lee. Connecting Evidence-Based Policing and Cybercrime. Policing: An International Journal 43: 198–211. https://doi.org/10.1108/PIJPSM-07-2019-0107
28. Kshetri, Nir. 2016. Cybercrime and Cybersecurity in India: Causes, Consequences and Implications for the Future. *Crime Law and Social Change* 66:313–338. https://doi.org/10.1007/s10611-016-9629-3
29. Kumar, Kundan, and Verma Naresh Kumar. 2026. Cyber-Financial (Cy-Fi) Fraud in India: A Case Study of COVID-19 Induced Cybercrime in Mewat Region. *Journal of Asian and African Studies* 61:826–842. https://doi.org/10.1177/00219096241300444
30. Lee, Jin, Thomas J. Ree, George W. Holt, Burruss, and Adam M. Bossler. 2021. Examining English and Welsh Detectives' Views of Online Crime. *International Criminal Justice Review* 31:20–39. https://doi.org/10.1177/1057567719846224
31. Levi, Michael. 2017. Assessing the Trends, Scale and Nature of Economic Cybercrimes: Overview and Issues. *Crime Law and Social Change* 67:3–20. https://doi.org/10.1007/s10611-016-9645-3
32. Lusthaus, Jonathan. 2024. *Annual Review of Law and Social Science* 20:369–385. https://doi.org/10.1146/annurev-lawsocsci-041822-044042. Reconsidering Crime and Technology: What Is This Thing We Call Cybercrime?.
33. Mayer, Jonathan. 2016. Cybercrime Litigation. *University of Pennsylvania Law Review* 164:1453–1507.
34. MHA (Ministry of Home Affairs). 2024. Rajya Sabha Unstarred Question No. 233, Answered on 27 November 2024, Annexures I–II. New Delhi: Government of India. Available online: https://www.mha.gov.in/MHA1/Par2017/pdfs/par2024-pdfs/RS27112024/233.pdf (accessed on 5 October 2026).
35. MHA (Ministry of Home Affairs). 2025a. Lok Sabha Unstarred Question No. 452, Answered on 2 December 2025, Annexures I–III. New Delhi: Government of India. Available online: https://www.mha.gov.in/MHA1/Par2017/pdfs/par2025-pdfs/LS02122025/452.pdf (accessed on 5 October 2026).
36. MHA (Ministry of Home Affairs). 2025b. Lok Sabha Unstarred Question No. 438, Answered on 2 December 2025, Annexures I–II. New Delhi: Government of India. Available online: https://www.mha.gov.in/MHA1/Par2017/pdfs/par2025-pdfs/LS02122025/438.pdf (accessed on 5 October 2026).
37. Mhavan, Neeta Vaibhav, and Priya Singh. 2025. Safeguarding Children in the Digital Age: Examining India's Cyber Laws and Child Protection Policies. In *Child Protection Laws and Crime in the Digital Era*, 305–331. Hershey: IGI Global. https://doi.org/10.4018/979-8-3373-5132-2.ch013
38. NCRB (National Crime Records Bureau). 2025. Crime in India 2023, Volume II, Tables 9B.4 and 9B.6. New Delhi: Ministry of Home Affairs. Available online: https://data.opencity.in/dataset/crime-in-india-2023 (accessed on 5 October 2026).

39. NCRB (National Crime Records Bureau). 2026. Crime in India 2024. New Delhi: Ministry of Home Affairs. Available online: https://www.ncrb.gov.in/uploads/files/2CrimeinIndia2024-VolumeII.pdf (accessed on 5 October 2026).
40. Nguyen, Trong, Tung Vu Van, Truong, and Lai Cuong Kien. 2022. Legal Challenges to Combating Cybercrime: An Approach from Vietnam. *Crime Law and Social Change* 77:231–252. https://doi.org/10.1007/s10611-021-09986-7
41. Nikkhah, Hamid, Jalal Reza, Varun Sarabadani, Grover, and Syed Shuva. 2026. A Review of Cybercrime Research: Synthesis and Future Directions. *Information & Management* 63:104369. https://doi.org/10.1016/j.im.2026.104369
42. Paramasivan, Kandaswamy, Akanksha Jaiswal, and Ameeta Fernando, Nandan Sudarsanam. 2026. Victim-Centric Approach to Financial Cybercrime: Exploring Vulnerabilities in the Indian Digital Landscape. *Humanities and Social Sciences Communications* 13:1411. https://doi.org/10.1057/s41599-026-07906-5
43. Paramasivan, Kandaswamy, Sriram Ravichandran, and Anusha Kumar. 2025. and Nandan Sudarsanam. Combating Cybercrime in India's Digital Age: Prediction and Prioritisation. Paper presented at the 2025 Cyber Awareness and Research Symposium (CARS). https://doi.org/10.1109/CARS67163.2025.11337835
44. PIB (Press Information Bureau). 2025. Cyber Crime Cases and Forensic Capabilities. PRID 2198253, 3 December 2025. New Delhi: Ministry of Home Affairs. Available online: https://www.pib.gov.in/PressReleasePage.aspx?PRID=2198253 (accessed on 5 October 2026).
45. Podsakoff, Philip M., B. Scott, Jeong-Yeon MacKenzie, Lee, and Nathan P. Podsakoff. 2003. Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies. *Journal of Applied Psychology* 88:879–903. https://doi.org/10.1037/0021-9010.88.5.879
46. Rai, Neha, and Chander Mohan Gupta, Gagandeep Kaur. 2026. Bridging Legislative Gaps: Evaluating the Role of Ethical Hackers in Investigating Financial Cybercrimes under India's Information Technology Act. *Lecture Notes in Networks and Systems* 1915:187–205. https://doi.org/10.1007/978-3-032-21901-5_16
47. Rakha, Naeem Allah. 2024. Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. *Mexican Law Review* 16:23–54. https://doi.org/10.22201/iij.24485306e.2024.2.18892
48. Rawandale, C. J., M. Manish, Deshpande, and Vinayak P. Rajadhyaksha. 2018. Banking on Online Banking: Digital Identity Theft in Banking Transactions—A Victim Oriented Case Analysis. Paper presented at the 2018 International Conference on Advances in Communication and Computing Technology (ICACCT), pp. 240–44.
49. Roy, Neha Chhabra, Sreeleakha Prabhakaran. 2023. Internal-Led Cyber Frauds in Indian Banks: An Effective Machine Learning-Based Defense System to Fraud Detection, Prioritization and Prevention. *Aslib Journal of Information Management* 75:246–296. https://doi.org/10.1108/AJIM-11-2021-0339
50. Sarkar, Gargi, Venkata Sai Charan Putrevu, and Shukla Sandeep Kumar. 2026. Understanding Jamtara Cybercriminals: Poverty, Opportunity, and the Rise of Organized Criminal Networks. *Humanities and*

Social Sciences Communications 13:1365. https://doi.org/10.1057/s41599-026-07703-0

51. Shetty, Anoop A., and K. Venkatesh Murthy. 2023. Investigation of Card Skimming Cases: An Indian Perspective. *Journal of Applied Security Research* 18:519–532. https://doi.org/10.1080/19361610.2021.2024049
52. Suseno, Sigid, Ahmad M. Ramli, Ranti Fauza Mayana, Tasya Safiranita, and Bernadette Aurellia Nathania Tiarma. 2025. Cybercrime in the New Criminal Code in Indonesia. *Cogent Social Sciences* 11:2439543. https://doi.org/10.1080/23311886.2024.2439543
53. Vaz, Andrea, Arruda, and Pedro de Oliveira Santos Junior. 2026. Alexia Ketlyn Soares dos Santos, and. The Efficacy of Penalty Enforcement for Cybercrimes Committed Using False Identity on the Internet. Derecho Penal y Criminología 47: 119–36. https://doi.org/10.18601/01210483.v47n123.06
54. Verma, Harish, Shambhu Kumar, Simmi Shukla, Bhumika Pal, Dhananjay Kumar Sharma, Priti Mishra, and Chaudhari, Poonam Pant. 2026. Cybersecurity Laws and Their Enforcement in India: Insights from Machine Learning Driven Case Analysis. *Lecture Notes in Networks and Systems* 1709:67–80. https://doi.org/10.1007/978-3-032-10199-0_5
55. Whelan, Chad, James Martin, Benoit Dupont, and Diarmaid Harkin. 2026. The Name of the Game': Policing Perspectives on Cybercrime Disruption. *Police Practice and Research* 27:289–309. https://doi.org/10.1080/15614263.2025.2523522
56. Zhang, Yu, Haoyun Dong. 2023. Criminal Law Regulation of Cyber Fraud Crimes—From the Perspective of Citizens' Personal Information Protection in the Era of Edge Computing. *Journal of Cloud Computing* 12:64. https://doi.org/10.1186/s13677-023-00437-3

Figures

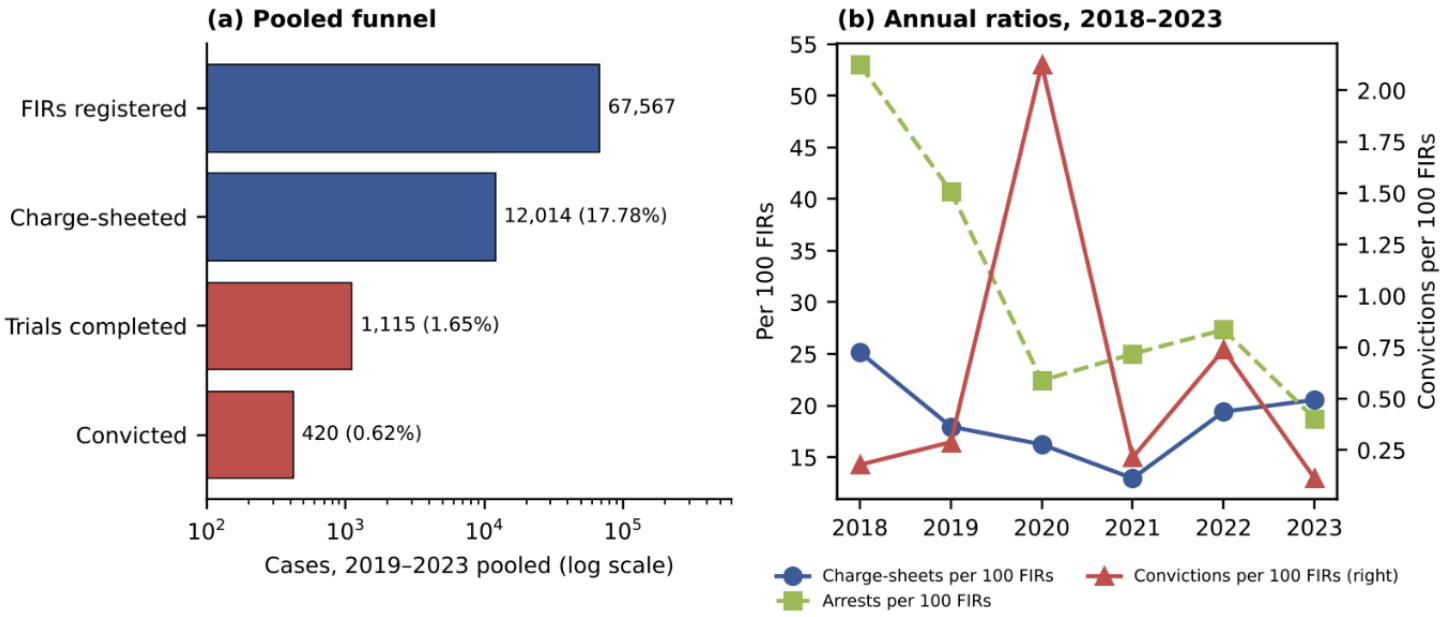


Figure 1

Decline in cyber crimes committed for financial gain in India: (**a**) consolidated diagram of FIRs to convictions, 2019–2023 (log scale; percentages show shares of FIRs); (**b**) charge-sheets, arrests and convictions per 100 FIRs, 2018–2023. Source: prepared using data from MHA (2024, 2025a).

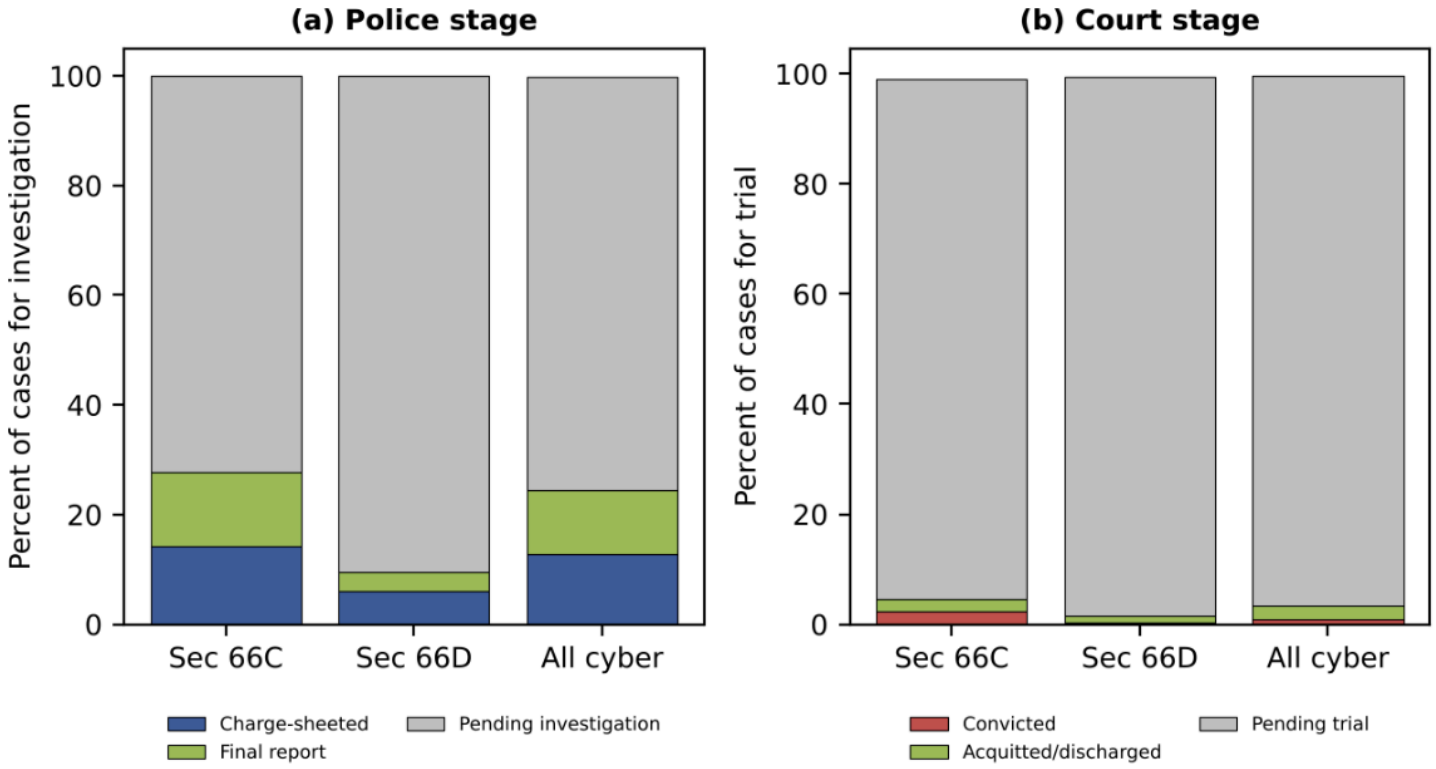


Figure 2

Disposal of Section 66C, Section 66D and all cyber crime cases at the police and court stages, 19 metropolitan cities, 2023. Source: computed from NCRB (2025), Tables 9B.4 and 9B.6.

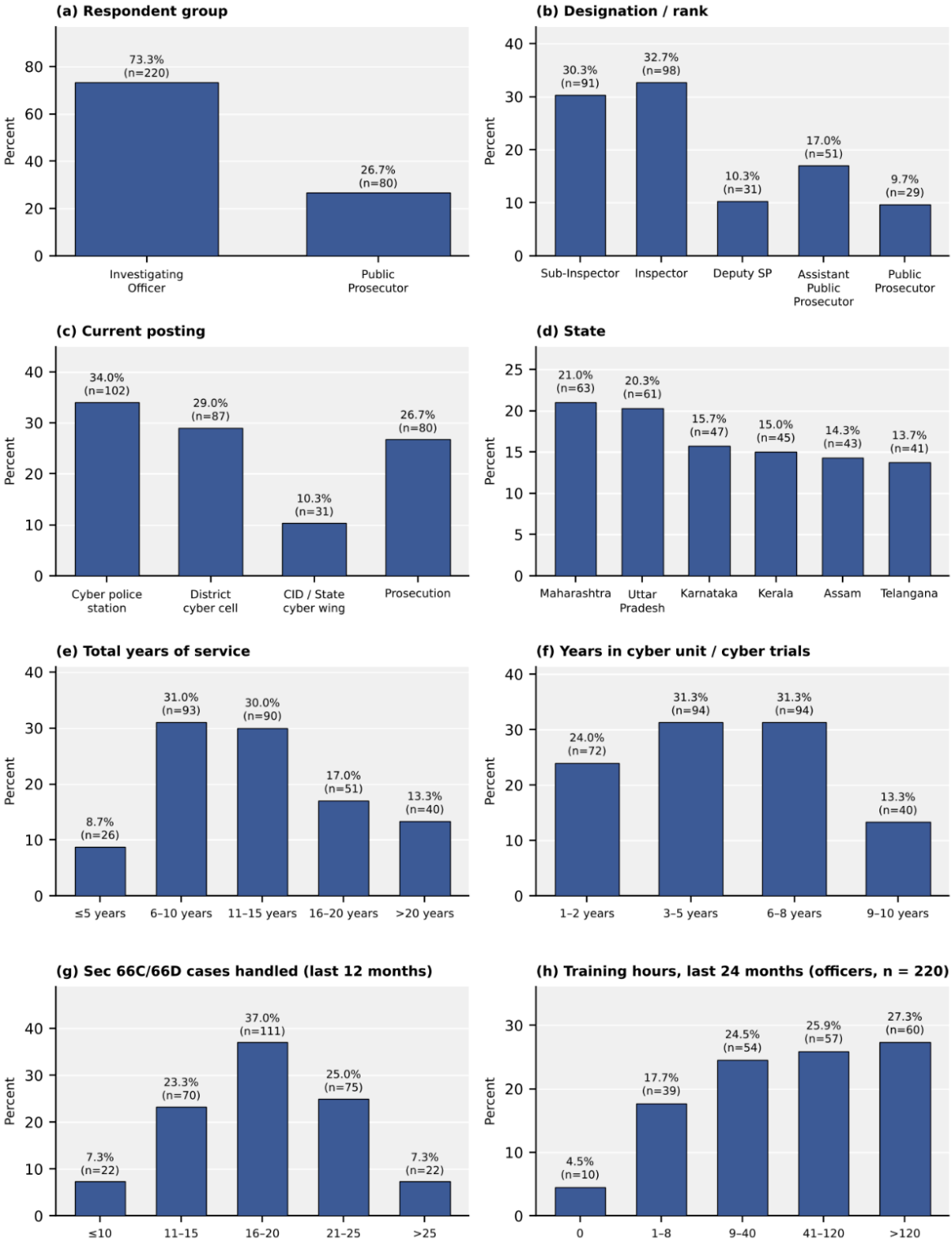


Figure 3

Profile of respondents (N = 300): (**a**) respondent group; (**b**) designation; (**c**) posting; (**d**) State; (**e**) years of service; (**f**) years in a cyber unit or handling cyber trials; (**g**) Section 66C/66D cases handled in the previous 12 months; (**h**) formal cyber crime training in the previous 24 months (officers, n = 220). Bars show percentages; counts are given in parentheses.

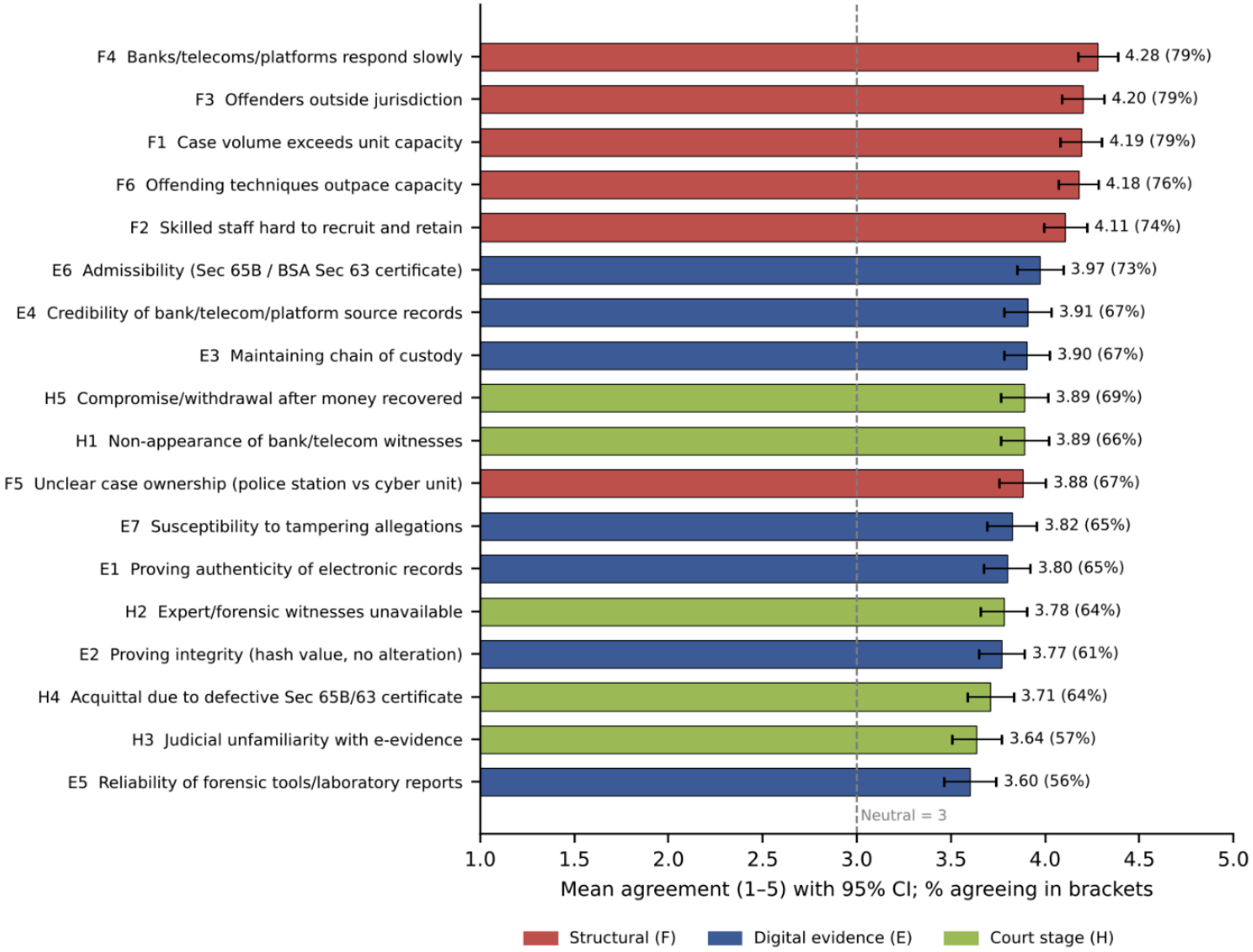


Figure 4

Perceived impediments to the prosecution of identity theft, ranked by mean agreement (N = 300). Error bars show 95% confidence intervals; the dashed line marks the neutral midpoint.

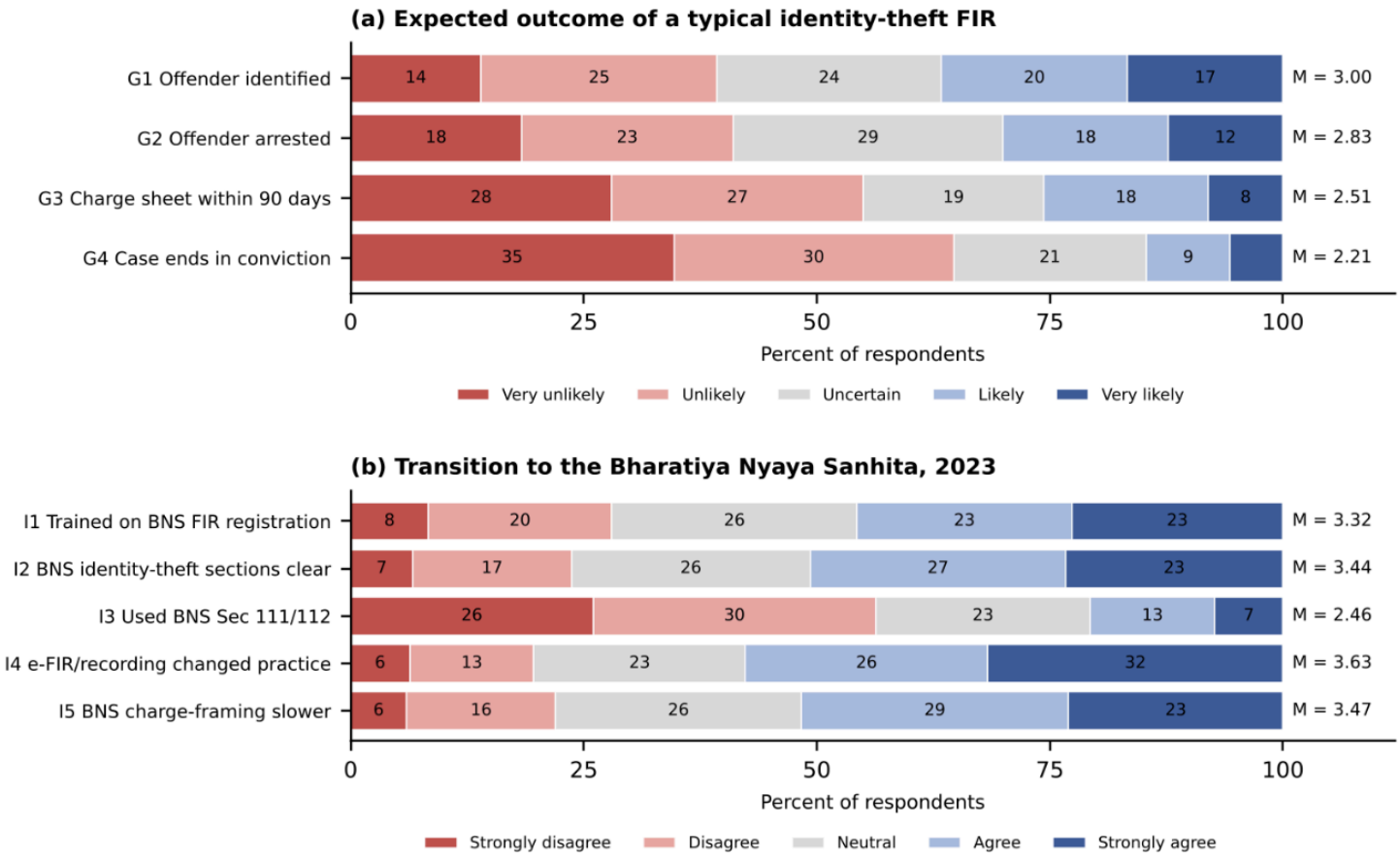


Figure 5

Distribution of responses (%): (**a**) expected outcome of a typical identity-theft FIR at four stages; (**b**) experience of the transition to the Bharatiya Nyaya Sanhita, 2023 (N = 300).