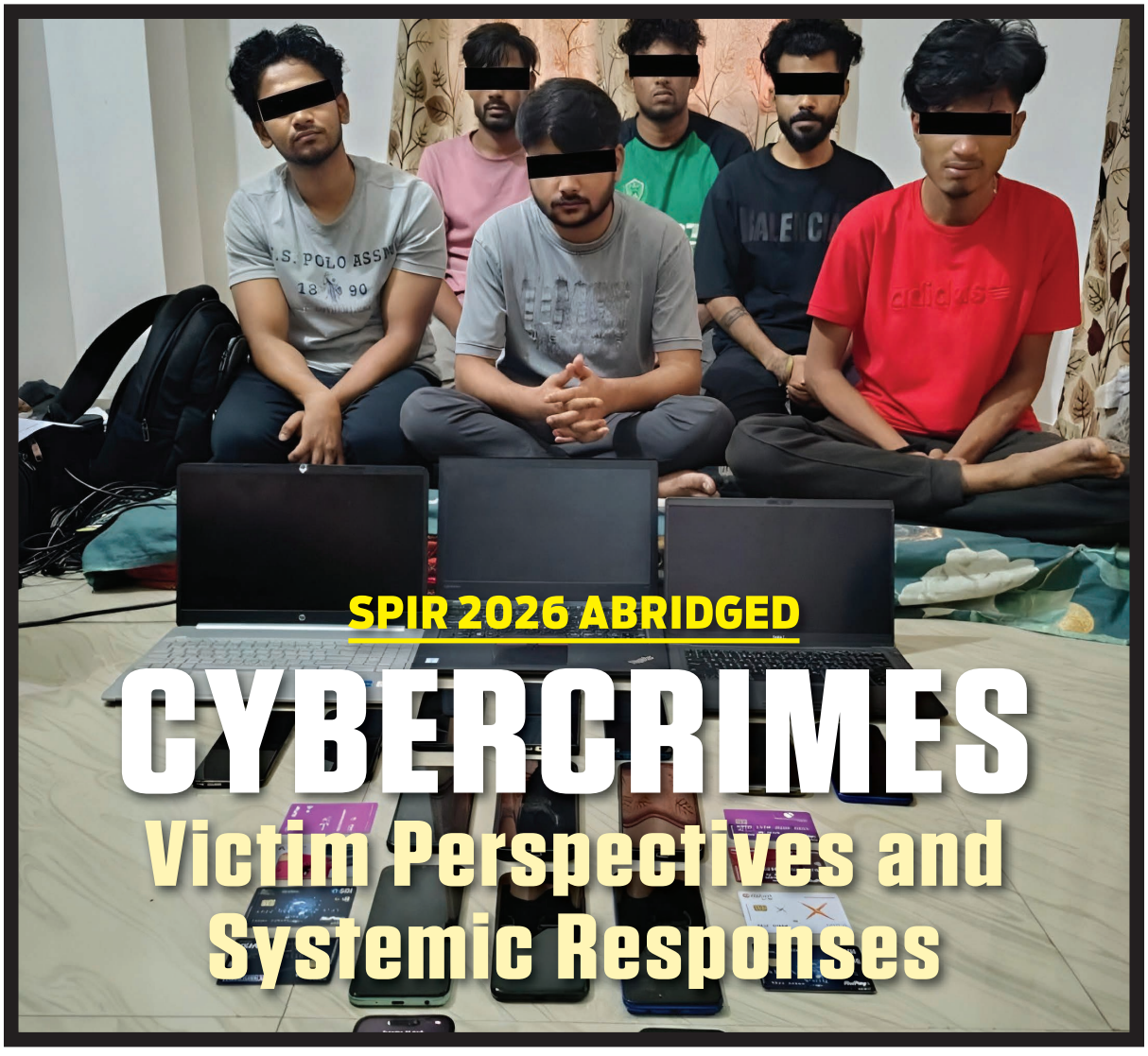
Vol. XLV No. 3 July-September, 2026

COMMON CAUSE

www.commoncause.in

POLICY-ORIENTED JOURNAL SINCE 1982



SPIR 2026 ABRIDGED

CYBERCRIMES

Victim Perspectives and Systemic Responses

Editorial: Human Cost of Cybercrimes	03	Common Cause Events	25
Perspectives of Victims and Experts	04	Digital Hygiene and Security Habits	26
Online Exposure and Its Drawbacks	08	How Competent Are Our Institutions?	30
Running From Pillar to Post	13	Recommendations	34
Banks Are the First Line of Defence	16	Common Cause Case Updates	37
Excerpts from Panel Discussion	19		

Price: Free distribution to members Regn No. 39331/1982



Common Cause is in the vanguard of India's anti-corruption movement and the fight for stronger public institutions since the 1980s. We make democratic interventions through PILs and bold initiatives. Our landmark PILs include those for the cancellation of 2G licenses and captive coal block allocations, against the criminalisation of politics, for Internet freedom and patients' right to die with dignity. Please visit commoncause.in for more information on our mission and objectives. We also run special programmes on police reforms and cleaner elections.

Common Cause runs mainly on donations and contributions from well-wishers. Your support enables us to research and pursue more ideas for a better India.

Now you can donate using our new payment gateway.

You may also deposit directly into our bank account (details are given below) and send us an email at commoncauseindia@gmail.com, providing information such as donor's name, address and PAN number for issuance of the donation receipt.

Name: Common Cause
Bank: IndusInd Bank
Branch: Vasant Kunj, New Delhi
S.B. Account No.: 100054373678
IFSC Code: INDB0000161
Address: Common Cause,
Common Cause House, 5, Institutional Area,
Nelson Mandela Marg, Vasant Kunj, New Delhi - 110070
(Phone numbers: 011 26131313 and 45152796)

Designed at GENESIS genesisadvt@hotmail.com 9810033682

HUMAN COST OF CYBERCRIMES

Status of Policing in India Report 2026

Cybercrimes have become inescapable. In one way or another, they have affected us, our friends or our relatives. These ghostly crimes have not only stolen our data, emptied our bank accounts, or tarnished reputations, but they have also shattered our sense of safety and security in cyberspace. What makes our fight particularly daunting is that its shadowy ecosystem transcends cities, jurisdictions, and countries.

A good way to begin the fight against this menace is to understand the modus operandi of cybercriminals, the nature of our vulnerabilities and the state of our preparedness. The latest Status of Policing in India Report (SPIR 2026) tries to do exactly that. Its title "Cybercrime – Victim Perspectives and Systemic Responses" is self-explanatory. For this research-based study, we have defined cybercrimes as crimes or illegal actions committed in the cyber sphere, using a networked device. It was launched on September 24, 2026, at the India International Centre, New Delhi.

Soft copies can be downloaded from our website, commoncause.in

As is the practice, we have dedicated this issue of your journal to its findings and recommendations. SPIR 2026 is based on all-India surveys, in-depth interviews and focus group discussions with domain experts around the following types of cybercrimes: (a) where someone impersonates you or illegally breaks into your devices, (b) when someone is manipulated psychologically through "social engineering" or is arrested digitally, and (c) when someone is targeted for trolling, cyberbullying, or online sexual abuse.

We surveyed over 8000 citizens in 16 states of India, including victims and those who assisted them. The qualitative analysis is based on interviews with victims and experts. The surveys cover the lower, middle and higher-income localities in selected urban and rural areas. The study focused on the nature and experiences of victims across offences such as online fraud, digital arrests, trolling, bullying, identity theft, and online sexual harassment.

The SPIR 2026 tries to show how we are targeted, our weaknesses and lived experiences, and how the authorities—the police and the banking system— respond when we need them most. We have tried to include incidents of abuse and cyberstalking of women and targeting of senior citizens. We understand that the ever-changing nature of cybercrime makes it an under-researched topic. The SPIR 2026 tries to fill that gap.

Many of our esteemed members and well-wishers attended the SPIR launch event. But for the benefit of those who could not be with us, we have presented here a summary of the chapters and their key findings. We have also presented excerpts of the speeches and an interactive panel discussion at the event. The topic was "Cybercrimes: Victims, Responses, Accountability." The illustrious panel comprised Retired IPS officer and cybersecurity expert, Mr Sanjay Sahay; gender specialist and social researcher, Dr Ranjana Kumari; CEO and co-founder of DeepStrat, Mr Saikat Datta; and digital rights activist and founder of Medianama, Mr Nikhil Pahwa.

The SPIR 2026 showed that police are particularly harsh and unhelpful to victims from poor and underprivileged backgrounds. We should be mindful that digital manipulations are also being used to polarise our world and weaponise our anxieties. UN human rights reports warn that malicious use of digital tech is undermining free speech and electoral integrity. We hope to take up some of these issues in the future.

Your feedback, comments or suggestions are welcome at contact@commoncause.in

Vipul Mudgal
Editor

MAPPING THE CYBERCRIME EXPERIENCE

Perspectives of Victims and Experts

Public discourse on cybercrime often centres on statistics documenting the proliferation of such offences, particularly digital financial fraud. The focus is often on the scale of cybercrime and the monetary losses it causes to victims and the country as a whole. However, a crucial yet relatively underexplored dimension is the lived experience of those directly affected by these crimes. Amid the dominant technical and financial discourse around cybercrimes, there is an emerging need to examine the experiences of victims of both financial and non-financial cybercrimes. While the crime itself can have far-reaching consequences, the ordeal of navigating the legal system and other procedures in its aftermath is equally important to understand.

Against this backdrop, the *Status of Policing in India Report 2026: Cybercrime—Victim Experiences and Systemic Responses* examines cybercrime from the perspectives of those most directly affected—victims and the general public. To understand not only the nature and prevalence of cybercrime but also the preparedness of institutions to respond to it, the study combines a large-scale survey of the general public (presented in Chapters 3 to 9 of the report), with in-depth interviews with cybercrime victims and domain experts (presented in Chapters 1 and 2 of the report).

This article presents key findings and excerpts from the qualitative interviews and the focus group discussion (FGD) with cybercrime victims and experts. It draws on qualitative insights gathered through detailed one-on-one interviews and a FGD. It brings together findings from open-ended conversations with 37 respondents, including domain experts, cybercrime victims, individuals who assisted victims, and family members of people accused of cybercrime.

A detailed account of the findings is presented in Chapters 1 and 2 of the report.

Modus Operandi of Cybercrimes

- Cybercrime perpetrators rely heavily on "social engineering" to commit crimes, using deception, manipulation, coercion and threats to gain access to sensitive information or personal devices. Majority of the financial cybercrime victims interviewed unknowingly shared sensitive information or transferred money under threat or deception. Of the 13 financial cybercrime victims who were interviewed, only two claimed that their accounts were accessed/hacked without them sharing any information with a third party or without any known sources of data leaks.

- There are organised networks running both the financial and non-financial cybercrimes. Databases of leaked sensitive information are available for easy purchase, along with "kits" selling mule accounts and fake SIM cards.

- Many of the non-financial cybercrimes, such as cyberbullying, also function in a highly organised setup. The victims described coordinated networks operating multiple fake social media accounts operating from not just across the country, but also internationally. A sting operation conducted by a news agency found that the network relied on multiple "sleeper cells" operating across various locations, where members associated with the network would provide on-ground information.

- In most cases of Non-Consensual Intimate Image (NCII) abuse, such as revenge porn, morphed images and

deepfakes, the perpetrator is someone known to the victim, according to experts.

Reporting of Cybercrime Cases

- Many cases of cybercrimes go unreported because of the social stigma and fear of public embarrassment, lack of trust in the authorities, lack of awareness about the redressal mechanisms and the feeling that the case will not be taken seriously by the authorities.

- In a few cases, victims are unwittingly made complicit in the crime, which inhibits reporting. A victim of a betting app fraud, who lost about Rs. 2.5 lakh, did not report the case to the police or any other authority since he had invited his friends and relatives to invest in the app, unaware that it was a fraud. He was afraid that he would also be implicated if he reached out to the authorities.

- Cybercrime experts noted that under-reporting is significantly more common in cases of non-financial cybercrimes, even though they are more pervasive. Cases of defamation, sextortion, impersonation, cyberbullying and NCII abuse are very rarely reported because of the reputational harm to the victim, the anonymity of the perpetrator and lack of adequate redressal mechanism.

- Victims and experts noted that the online police complaint mechanism was cumbersome to navigate and lack of clarity regarding the investigation that followed. Many did not receive any communication from the police other than an automated acknowledgement number.

- Victims also do not have clarity on the steps that should be taken by law enforcement after a complaint has been made on the portal. Of the 16 victims of cybercrimes that were interviewed, about half (nine) reported their case using the online portal or the centralised helpline number. While a majority of these victims got a call back after complaining online, in at least four of these cases, the victims did not receive any call back or update on their cases even after months, and in some cases, years.

> ***"Many of the non-financial cybercrimes, such as cyberbullying, also function in a highly organised setup. The victims described coordinated networks operating multiple fake social media accounts operating from not just across the country, but also internationally"***

Victims' Experience with the Police

- Most of the victims who visited cyber police stations or units felt that the staff was polite and helpful. However, with victims from poor backgrounds, the police were reportedly rude, dismissive and abusive. One of the victims, son of a domestic worker, recalled the police being abusive towards him and his parents, and refusing to register an FIR.

- FIRs are not commonly registered in cybercrime cases. Of the 15 victims who complained to the police either online or in person, an FIR was registered in six cases. Two of these were automatic FIRs, and in at least two other cases, the victims reached out to persons of influence to get the FIR registered.

- An investigating officer (IO) from a cybercrime police station in Delhi informed the research team that of the approximately 15,000 cybercrime complaints registered in their jurisdiction in the previous year, just about 250 cases were converted into FIRs. He highlighted the lack of human resources and the non-investigative load on IOs as the primary reasons for the low conversion rate.

- Victims had no information about any investigation into the crime being done by the police. The police often cited

jurisdiction problems and lack of coordination between state police departments as the primary deterrents against conclusive investigations.

- Victims of financial cybercrimes overwhelmingly felt that there was a lack of proper communication and coordination between the banks and the police. Several victims reported having to act as a liaison between the banks and the police and pass on relevant information from one institution to the other for timely action on their cases.

- In cases of online gender-based violence, experts highlighted the police apathy towards such crimes and their tendency to blame the victims. The focus of the police is often on "settling" the cases, urging victims to come to a compromise with the perpetrators.

- Amongst the ten respondents who rated their experience with the police, the average rating given to the police was 2.4 out of five.

Victims' Experience with the Banks

- Victims of financial cybercrimes and experts overwhelmingly felt that the banks refused to take accountability, or assist the victim through the recovery process. Barring one case, in all other interviews with financial fraud victims, the banks maintained that the victims "*collaborated*" with the fraudster.

- In at least two cases of financial frauds interviewed, despite timely reporting by the victim, the banks were negligent in freezing their accounts promptly, which led to further loss to the victim.

> ***"Most victims described litigation as a long and uncertain process that requires significant time, financial resources and persistence."***

- Five of the financial cybercrime victims were of the opinion that banks were complicit in cybercrimes. A few other pointed to the lack of data security and vigilance on the part of the bank, which made the customers vulnerable to cybercrime attacks. The interviewed cybercrime experts, retired and serving police officers, were also strongly of this opinion. Several respondents highlighted the common instances of data leaks in the banks which are not sufficiently addressed. These leaks, they said, are caused both due to inadequate security systems and the direct complicity of some banking officials.

- Amongst the six victims who rated their experience with the banks, the overall rating was a poor one out of five.

Victims' Experience with the Courts

- Most victims described litigation as a long and uncertain process that requires significant time, financial resources and persistence. Out of the 16 cybercrime victims, only four victims employed legal representation and pursued litigation through the courts. A victim explained that pursuing a court case would involve paying lawyers, attending repeated hearings and spending additional money without any certainty of recovery.

- Older victims may experience additional vulnerabilities when engaging with complex legal and institutional systems. A senior citizen respondent described considerable difficulty navigating legal procedures and assessing the reliability of legal assistance.

- Victims who entered the judicial process consistently spoke about delays. Their frustration stemmed not simply from the passage of time, but from the absence of visible progress despite repeated hearings

Case Outcomes

- **Digital arrest cases:** Amongst the three digital arrest victims interviewed, only one suffered an actual financial loss. The

victim was able to register an FIR and 11-12 mule account holders linked to the racket were arrested. But he was unable to recover a majority of the amount lost. He recovered only Rs 5 lakh of the Rs 65 lakh lost.

- **Other financial fraud cases:** Of the ten respondents who lost money through financial frauds (other than digital arrest), five were able to recover a partial amount at either the bank level, or through court or RBI orders, and one was able to recover the full amount through their bank.

- **Cyberbullying cases:** The two cyberbullying victims interviewed approached a senior-level police officer through a personal connection. A complaint was taken, but FIR was not registered. The offensive social media content was taken down over a six-month period, but no further police investigation or action was taken.

Factors Influencing Case Outcomes

- **Bribes to the police:** Only one victim suspected that the police-appointed lawyer and the police pocketed the amount paid by him for a court order towards partial release of the lost money. Rest of the victims did not report having to pay any bribe to the police.

- **Contacting persons of influence:** In both financial as well as non-financial cybercrime cases, informal contacts with persons of influence played a major role in the case being taken seriously at various stages—registration of FIR, police investigation and action, complaint to the RBI ombudsman and recovery of money. Of the six financial fraud victims who recovered money partially or fully, three used personal connections, and one was a high net-worth individual who was assisted by the bank.

Impact of Cybercrimes

- Several victims described facing stress, trauma and depression due to the cybercrime and the complaints procedure that followed. One of the victims had a miscarriage. Another had to leave her profession and move to a different country. One of the victims, a senior citizen, lost financial autonomy and now relies on her children to withdraw cash and manage her financial dealings.

- For some of the victims, the trauma stems not only from the cybercrime incident, but also the mentally and physically taxing legal procedures that follow. A then-minor victim of sextortion reported facing lasting depression and trauma due to the police's rude behaviour towards him and his family.

Accounts of Families of Accused and Others

- The study includes interviews with family members of two persons who have been accused in separate cases of cybercrimes. In one of the cases, the accused was approached by a bank official with an offer of a low-interest loan. An account was opened under his name in that regard, and unknown to him, was being used as a mule account for cybercrimes. In the other case, an 18-year-old was convinced by a co-worker to open a mule account and supply a fake SIM card in exchange for Rs 5,000 *"now and then"*. Both the accused were in prison at the time of the interviews.

- Three other respondents reported having their bank accounts frozen due to an ongoing investigation, though they were not privy to the details of these cases. These respondents were neither victims nor accused, but had to liaison between the banks and the police to get access to their accounts.

- The three respondents whose bank accounts were frozen and the two accused persons were Muslim.

ONLINE EXPOSURE AND ITS DRAWBACKS

Digital Access Increases Risks of Digital Fraud

Your phone rings, a cheerful voice announces that a parcel is waiting for you. You do not remember ordering one. You conclude that it maybe someone in your house – them and their online shopping habits. An exasperated sigh later, you ask the caller to carry on, slightly annoyed at the one at home not letting you know about their parcels.

The cheerful voice continues. Your parcel was caught at customs. At times it only needs a small payment to be cleared, other times it has illegal items that are going to get you prosecuted. The fraudster's playbook is already in motion before you know it. Your name, your address, are recited back to you. Fear reaches your throat and opens it for your recital. Your family tree, your bank account, your workplace, all flow naturally to the "officer" who you have been transferred to now.

If this sounds familiar, you are in large company. In the *Status of Policing in India Report* 2026, we surveyed 8,306 people across 16 states and found that the fraudster's call is hardly a rare event. It is a common hazard of owning a phone.

This article delves into what we asked and learned in chapters 3 and 4 of the report. How often do these attempts reach people? What do they fear most? Do they feel targeted because of who they are? And who, in the end, actually falls victim?

Exposure to Cybercrime

Fraudsters are inventive. Their methods keep evolving and the novelty of their schemes casts a wide net in which victims are caught. Before the public realises such a net has been cast, it

Table 1: High-return investment and fake delivery scams are among the most frequently reported fraud attempts

Received a call/text message for	Many times	Sometimes	Rarely	Never
Investment opportunity, guaranteeing a high return	10	21	20	45
Delivery of a product you never ordered	8	25	20	44
Bank official asking for personal or account details	7	20	21	49
The phone number has been linked to illegal activities	6	17	16	56
An unknown number claiming to be your friend/ relative who is in urgent need of money	6	17	19	54
Call from police or someone in authority claiming that your friend / relative is in danger or has committed some crime	5	15	18	59

Note: All figures are in percentages. Rest did not respond. Question asked: "How often do you receive a call/text message – Delivery of a product you never ordered/ Phone number has been linked to illegal activities/ Bank official asking for personal or account details/ Unknown number claiming to be your friend/relative who is in urgent need for money/ Police or an authority claiming a friend or relative is in danger or committed a crime – many times, sometimes, rarely, or never?"

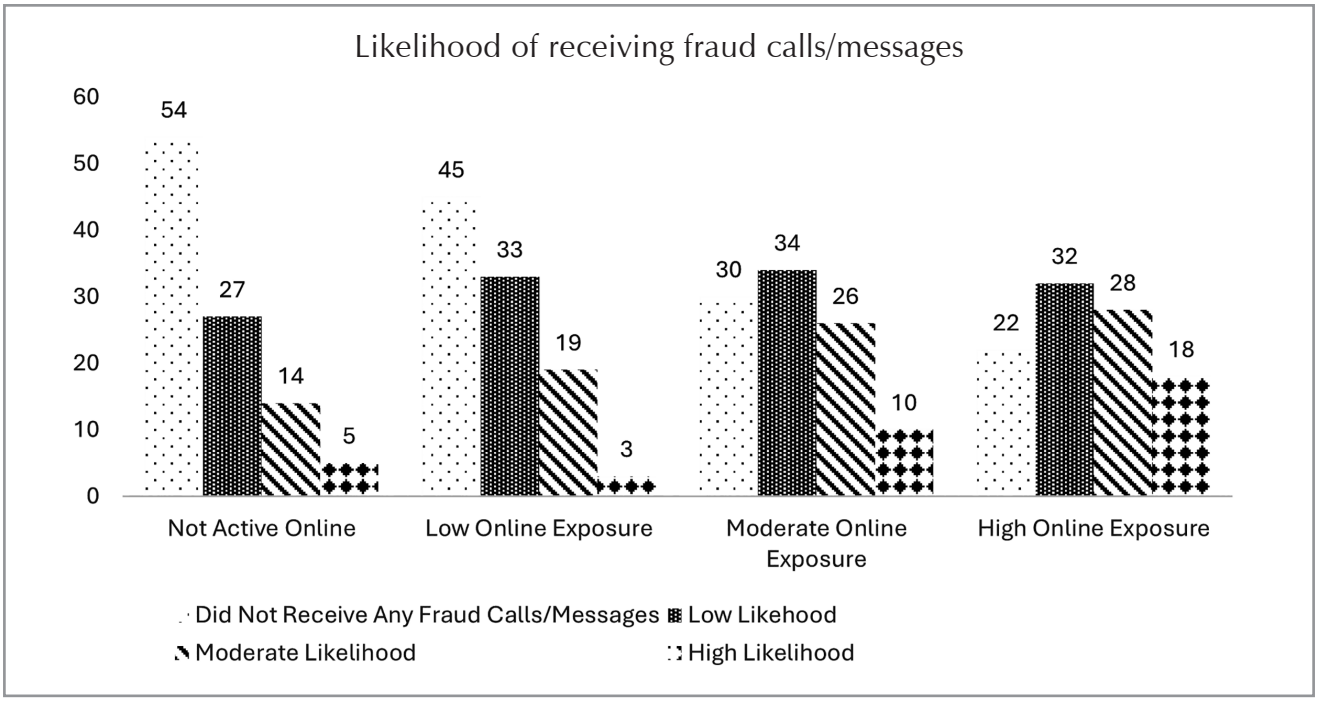
is reeled in and another takes its place. So, we asked respondents how often they come across such fraud attempts. One in three respondents had received fake calls about delivery of products they never ordered (33 per cent – combining "many times" and "sometimes"). A similar proportion encountered high-return investment scams (31 per cent – combining "many times" and "sometimes"). More than one in four (27 per cent) had received calls from individuals impersonating bank officials and asking for personal or account details. The frequency of exposure to other methods are given in Table 1.

When we look at exposure to cybercrime by class, the middle and high-income groups report more frequent scam calls/texts. For instance, about two in five (37 per cent) of those belonging to the middle class and over one in three (35 per cent) of those from the rich backgrounds frequently received fake delivery scam calls, compared to 29 per cent among the most economically disadvantaged. The pattern was similar across all types of fraud attempts.

Why might this be? There are two possible explanations. First, higher income groups may engage more actively in online transactions, investments, and e-commerce, while economically disadvantaged groups may interact differently with digital platforms, thereby making the former more vulnerable to cybercrime. Secondly, cyber fraud often involves profiling victims through publicly available information, bank and personal details, thus rendering those with greater financial means more vulnerable.

So, does deeper integration into the digital world increase one's exposure to fraudulent attempts? To answer this, questions on the respondent's usage of social media, online banking apps, and UPI were put together against the frequency of them receiving fraudulent calls/text. The answer was a resounding yes. Those who had the least internet activity were three times less likely than

Figure 1: Those who are more active on the internet are more likely to be exposed to fraud calls/messages



Note: All figures are in percentages. This is an index created using a battery of questions. These include questions on the frequency of using different modes of online payment, including UPI, NEFT/RTGS, cards, and payment wallets and another question on the frequency of receiving suspicious/fraud-related calls or messages, including fake deliveries, bank scams, emergency money requests, illegal activity claims, and fraudulent investment offers.

those with high online exposure to have a high likelihood of receiving fraudulent calls/text **(Figure 1)**. Over half (54 per cent) of those who were not active on the internet reported receiving no fraud calls/texts, compared to over a fifth (22 per cent) of those with high internet activity. Figure 1 also shows a steady climb: as online activity increased, so did the exposure to fraudulent calls/texts.

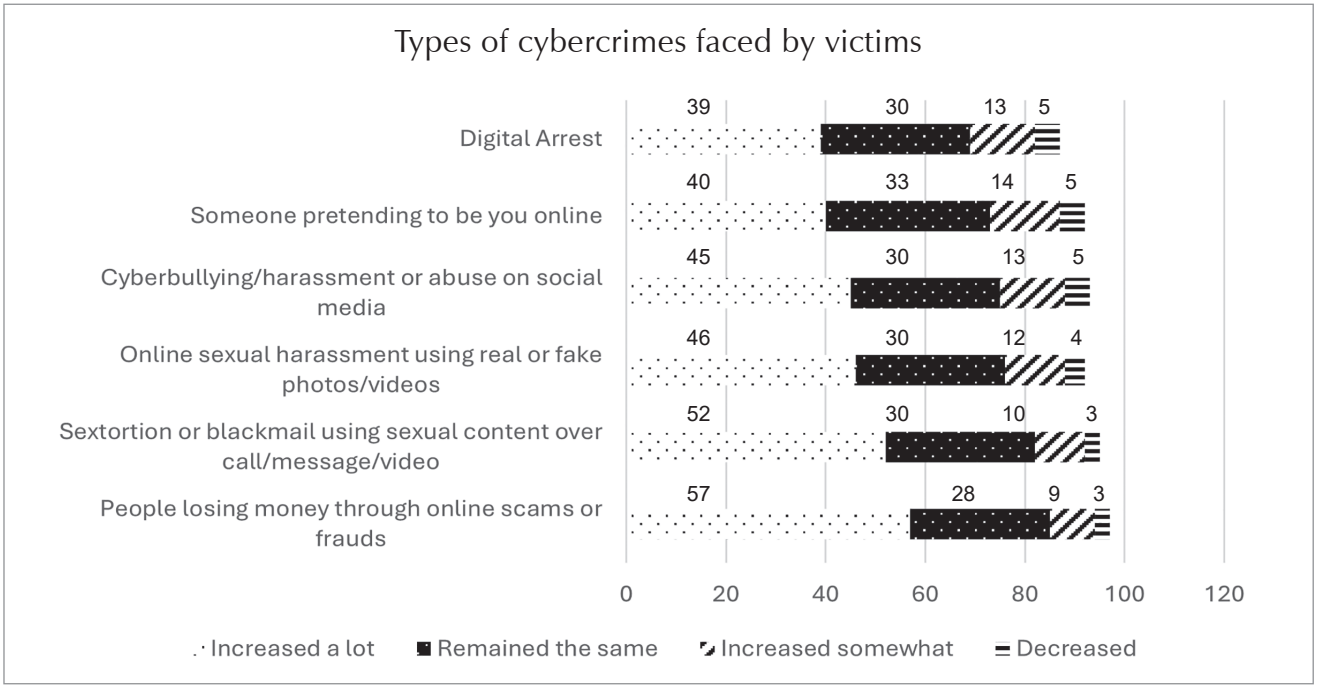
The same was observed for those who frequently use online payment services. About half (49 per cent) of those who do not use any online payment services reported never receiving any fraudulent calls/texts compared to only 14 per cent of those who use online payment services frequently. A quarter of those who frequently use online payment services reported a high likelihood of exposure to cybercrime attempts compared to only 6 per cent of those do not use online payment services. The incremental pattern was also the same, as usage of online payment services increased so did their exposure to fraudulent calls/texts.

Fear of Cybercrime

Fear of cybercrime was high across the board among respondents. People were most afraid of losing money through online fraud or scams, with over half (55 per cent) reporting high fear of being victimised. However, almost similar proportions were reported across other categories of cybercrime. Forty-seven per cent highly feared someone impersonating them online, one in two (51 per cent) highly feared identity theft (someone stealing and misusing personal IDs such as Aadhaar card), 49 per cent highly feared their devices being hacked, and the same proportion highly feared being recorded without their consent.

Women exhibited higher fear than men over all types of cybercrimes. They were also significantly more likely than men to feel vulnerable to online gender-based cybercrimes. Almost three in ten (29 per cent) women reported that they are very likely to be targeted online because of their gender, compared to two in ten (19 per cent) men.

Figure 2: Online scams and Sextortion or blackmailing cases are seen as rapidly growing threats



*Note: All figures are in percentages. Rest did not respond. *Option "Decreased" was a silent option.*
Question asked: "In your opinion, have the following increased a lot, increased somewhat, or remained the same, in the last two years – people losing money through online scams or frauds/ sextortion or blackmail using sexual content over call/message/ video/ online sexual harassment using real or fake photos/videos/ cyberbullying/harassment or abuse on social media/ someone pretending to be you online/ digital arrest?"

When asked about their vulnerability online owing to their caste, Scheduled Tribes reported being most vulnerable. Amongst internet users in general, those who have high internet activity were the most likely to have a high fear of cybercrimes. Nearly one in five (18 per cent) respondents felt that they were very likely to be targeted online due to their sexual orientation.

With fear this widespread, we also asked people about their perception on whether cybercrimes have increased a lot, somewhat increased, or remained the same? The majority felt that cybercrimes have increased a lot in the past two years. Almost three in five (57 per cent) felt that people losing money through online scams or frauds has "increased a lot" **(Figure 2)**. Over half (52 per cent) felt that sextortion or blackmail using sexual content has "increased a lot". Nearly half perceive a strong rise in online sexual harassment (46 per cent) and cyberbullying (45 per cent). Around four in ten see sharp increases in digital arrest scams (39 per cent) and impersonation (40 per cent).

Who are the Victims?

Of the 8,306 respondents, about 13 per cent (1,085 people) had been victims of cybercrime in the past two to three years. For those who weren't victims, we asked if they had closely helped someone who had been affected by cybercrime, and about 12 per cent (814 people) said that they have done so.

Table 2: Cybercrime victims report substantially higher exposure to frequent scam calls and messages

Received a call/text message for	Overall	Victims	Non-victims
Delivery of a product you never ordered	33	53	29
The Phone number has been linked to illegal activities	23	38	20
Bank official asking for personal of account details	27	46	23
An unknown number claiming to be your friend/relative who is in urgent need of money	23	44	19
Investment opportunity, guaranteeing high return	31	50	27
Call from police or someone in authority claiming that your friend/relative is in danger or has committed some crime	19	37	16

Note: All figures are in percentages. The figures here represent the combined responses of "many times" and "sometimes" categories. The categories of "many times" and "sometimes" have been combined as "frequently".

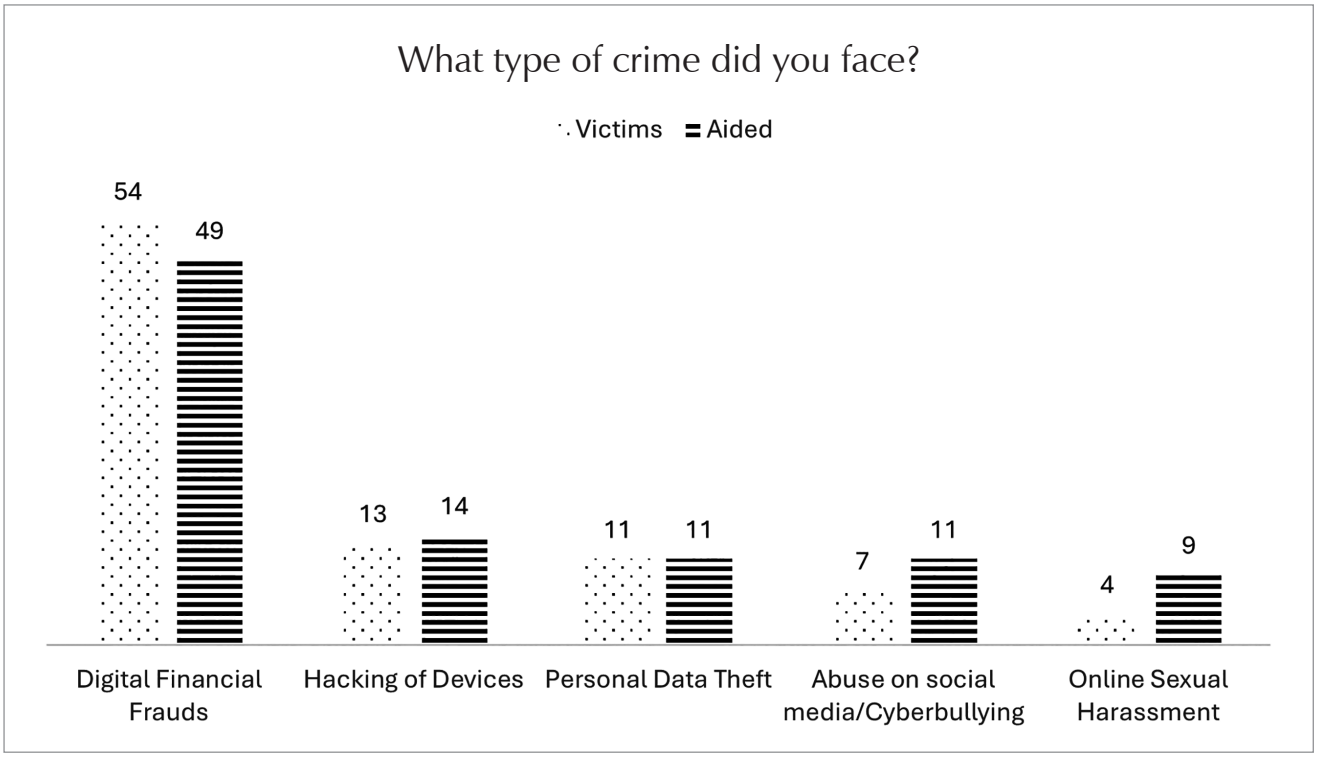
Victims reported higher exposure to fraudulent calls/texts than non-victims **(Table 2)**. Over half (53 per cent) of victims reported receiving a call/text about a product they never ordered, compared to about three in ten (29 per cent) non-victims. A similar pattern was found across all other types of fraud attempts as seen in **Table 2**.

Money was the Main Target

Digital financial frauds accounted for over half of the cases (54 per cent), followed by 13 per cent victimised by hacking of devices, one in ten (11 per cent) suffered personal data theft, 7 per cent by cyberbullying, and 4 per cent by online sexual harassment **(Figure 3)**.

The younger, richer and more educated respondents were the most vulnerable to digital financial frauds. One in six (16 per cent) respondents up to the age of 35 had been a victim of cybercrime, compared to 13 per cent of those aged 36-55 and 8 per cent of those above 56. Across class, 47 per cent of the most economically disadvantaged respondents had been a victim of digital financial

Figure 3: More than half of all cybercrimes involve digital financial frauds



Note: The rest did not respond or reported facing other types of crime. All figures are in percentages. Question asked: What type of crime did you face?

fraud, compared to 57 per cent of rich respondents. Across education levels, two in five (40 per cent) non-literate respondents were victims of digital financial frauds, compared to about three in five (59 per cent) college-educated respondents. It seems that the more access one has to the digital world, the more doors are created for a fraudster to knock on.

A Double-Edged Sword

Put the findings side by side and a pattern is hard to miss. The more people live online – through social media, banking apps and UPI – the more often a fraudster's call finds them. Victims were far more likely than non-victims to have received such calls (53 per cent against 29 per cent for the fake delivery call, for instance). And the people who might have the most goings on in their digital lives – the younger, the richer and the more educated – were the ones most vulnerable to digital financial fraud.

Fear is keeping pace. Over half of respondents (55 per cent) highly feared losing money to online fraud. Women feared more than men across every type of cybercrime, and most people believe the problem is getting worse, with almost three in five (57 per cent) saying that losing money to online scams has "increased a lot".

None of this is an argument for logging off. UPI, online banking and e-commerce have made everyday life easier for millions of people. The lesson is subtler: every convenience is also a door, and fraudsters, who are nothing if not inventive, are happy to knock on all of them. The wider the net they cast, the more it matters that someone is minding the doors, whether that is a bank, a platform, the police, or simply a person who pauses before pressing a button.

RUNNING FROM PILLAR TO POST

Travails of Cybercrime Redressal System

As India's digital economy expands, cybercrime is a growing threat that exposes individuals to financial losses, data theft, hacking, online harassment, and more. Yet, its impact extends beyond the immediate harm caused by the offence itself. What happens after the crime? A crime where the perpetrator is faceless, the loss is shapeless, but the impact is felt in all realness.

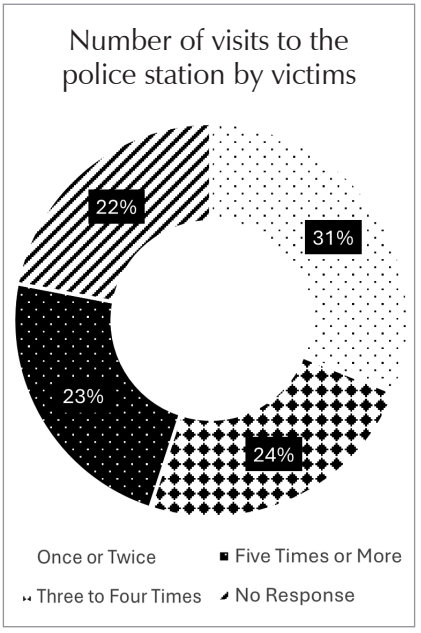
To answer this question, the *Status of Policing in India Report 2026* goes all across India, and asks 8,306 citizens in 16 states about how they use the internet, if they have been victimised by it, and where and how they sought justice. This article delves into the findings from *Chapter 5* of the report, which examines how victims navigate the redressal system, specifically the police and courts.

The Police Station Run

For most victims, the first instinct was to go to the police. Over half (51 per cent) complained to the police, and another 11 per cent said they initially went to the police, but did not pursue their case further. That leaves about a third (34 per cent) who did not complain at all. When asked why, nearly three in ten (28 per cent) said that they did not lose a big enough amount to complain, one in seven (14 per cent) found the complaint procedure difficult or complex, and one in ten were afraid of going to the police.

Complaints did not all begin at the same place. Half of those who complained (50 per cent) went to their local police station, while about a fifth (18 per cent) went to the cyber cell near them. The rest either called the local/cyber police station (10 per cent), cybercrime helpline (9 per cent), filed an online complaint (5 per cent), or complained to the bank (5 per cent). Those who walked into a police station then met the waiting room. About three in ten (30 per cent) waited for less than an hour, but the largest group (45 per cent) waited for about 2-3 hours. One in ten waited for 4-5 hours, and three per cent waited for more than five hours. It was also found that the most economically disadvantaged were three times less likely than the rich to wait for less than an hour. However, it must be noted that 46 per cent of the poor who visited the police station, did not report their waiting times.

Figure 4: Nearly a quarter of the victims visited the police station five times or more.



Note: All figures are in percentage.
Question asked: How many times did you have to visit the police station (local/cyber) during the investigation process?

As for the number of times people had to visit the police station, about a quarter (23 per cent) made five or more visits **(Figure 4)**, while two in five (41 per cent) people who assisted victims did the same. This points towards an enormous amount of leg work required of victims to seek justice. Rural victims were twice as likely (38 per cent) to visit the police station five or more times than urban victims (19 per cent).

Was it Worth the Trip?

Given all those visits, how did victims rate the experience? About a fifth (17 per cent) found it "very difficult" to get their complaint registered, while a quarter (25 per cent) found it "somewhat difficult". Economically weaker respondents were more likely to find the complaint registration process easy compared to their richer counterparts. Two in three (66 per cent) poor respondents found it easy to register their complaint, while over half of the rich respondents (55 per cent) reported the same. Across genders, women were more likely to rate the process easier than men (61 per cent and 54 per cent, respectively).

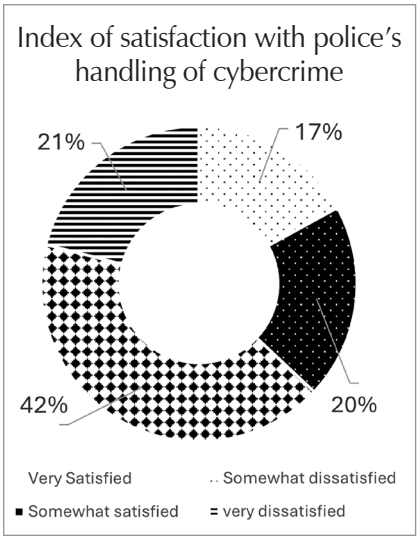
However, an easy start was not the same as an easy road to justice. To judge the whole journey, from registering the complaint to the resolution of the case, a composite satisfaction index was created **(Figure 5)**. It was found that about two in every three (63 per cent) victims were dissatisfied with the police's handling of their cybercrime. Two in five (42 per cent) victims were "somewhat dissatisfied", and a fifth (21 per cent) were "very dissatisfied". When seen across different social demographics, women, rural, and the most economically disadvantaged victims were the most likely to be dissatisfied with the police's handling of their case.

Greasing the Machine

A striking proportion – over a quarter of victims (27 per cent) – reported paying a bribe to the police **(Figure 6)**. Women were more likely to pay a bribe than men, with over one in three (35 per cent) women paying a bribe, compared to over one in five (22 per cent) men. But class made the starkest difference. Among those who paid a bribe to the police, over half (51 per cent) were the most economically disadvantaged, compared with 18 per cent of lower class, 17 per cent of middle class, and 12 per cent of rich victims.

For someone at the bottom of the economic ladder, any amount lost is significant, and getting it back is worth paying for. It is a sign of how exposed they are – easily exploited by the very people they turn to for help, and carrying the double burden of financial loss.

Figure 5: About two in every three victims are dissatisfied with the police handling of cybercrime.



Note: The index was created from these questions posed to victims: police helpline number for cyber complaints, online police portal for cybercrime, complaint registration process at cyber police station and investigation of cybercrimes by the police.

When seen across localities, one in three (36 per cent) rural victims paid a bribe to the police, compared to one in four (24 per cent) urban victims. Respondents were very hesitant to reveal the amount that they paid as a bribe, with about two in three (65 per cent) victims not disclosing the amount.

Figure 6: More than a quarter of the respondents who complained to the police paid a bribe to the police.



Following the thread of bribery to its logical end, the question whether recovery of lost money was possible or not, needs to be examined. Those who paid a bribe were three times (38 per cent) more likely to recover the full amount, compared to those who did not pay a bribe (12 per cent). An additional 16 per cent who paid a bribe achieved partial recovery, compared to 10 per cent partially recovering their money without a bribe. An overwhelming majority, three in four (75 per cent) victims who did not pay a bribe recovered none of their money, compared to about two in five (38 per cent) victims who paid a bribe. The difference is clear; you have got to spend money to find your lost money.

Bribes were not the only facilitators. More than a third of the victims (37 per cent) reached out to their personal network to nudge the police into investigating, and the majority (47 per cent) went straight to senior police officers. Women, victims from rural areas, and the most economically disadvantaged were more likely to leverage their personal network than their counterparts. Two in five women (41 per cent) had contacted someone in their personal network compared to a one in three (35 per cent) men. Almost the same proportion goes for rural victims (44 per cent vs 35 per cent). Across economic classes, 55 per cent of the poor respondents reached out to someone, compared to 30 per cent of the rich respondents.

Connections paid off. Over a quarter (28 per cent) of those who leveraged their personal connections fully

recovered their money, and less than a fifth (17 per cent) achieved a partial recovery, and a little less than half (48 per cent) recovered none of their money even with personal connections **(Figure 7)**.

The difference is although very stark when recovery is measured without any personal connections. Less than one in ten (8 per cent) were able to recovery the full amount without any personal connection, and the same proportion recovered a partial amount. Almost 72 per cent of those without any personal network, did not recover any money.

The message is clear: you need to oil the justice machine to get it working. You either grease the palms of the officers or have inroads with people in a position of influence over the police who can shift the gears in your favour.

Courts: The Last Piece of the Redressal Puzzle

One in five victims (20 per cent) had their cases progress to courts. Courts typically function as the last resort for victims, where a court order is necessary to get the lost funds transferred between banks, or in the words of bankers, get them "released" from the bank account they are "held" or "frozen". Courts also serve as a decisive step in the redressal process where the banks and victims can get tangible actions since the banks — as evidenced by interviews in the report — typically shrug off responsibility, derelict remedial actions for the fraud, or shift the blame onto the customer for being defrauded/ 'cooperating with the fraudster'.

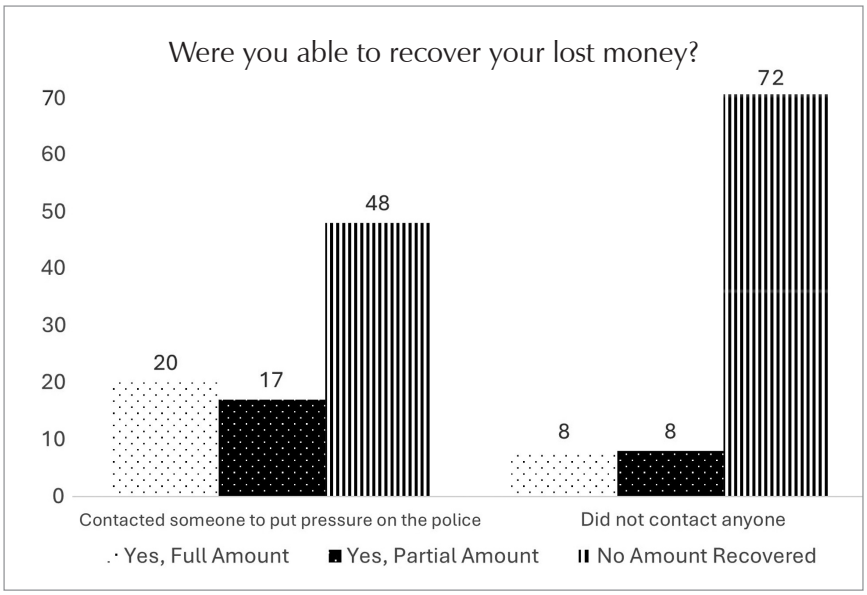
The victims whose cases went to court were mostly satisfied with the outcome, with 42 per cent being "completely satisfied", 26 per cent being "somewhat satisfied". However, 22 per cent did express complete dissatisfaction with the outcome of their case in court.

The Map to Justice is Bought

The pillars are all standing. India has police stations, cyber cells, helplines, banks and courts. The trouble is it is the victim who queues for hours, returns five times, asks a well-placed acquaintance to make the call, or slips money across a desk, all to recover what was theirs to begin with.

Our findings suggest the system, in practice, can reward the wrong things. Money and contacts seem to decide who gets their money back, and the people who are most vulnerable – women, rural residents and the poor – are often the ones paying the highest price to use it. The one pillar that appears to bear weight is the court, but only one in five victims ever reaches it, and even there not everyone goes home satisfied. A justice system should be one people can lean on, not something they have to prop up. Too many cybercrime victims hold up the pillar with their time, money and contacts, and still wonder where the post is. Until the first door a victim knocks on opens as readily as the last, or it is the only door they have to knock, being sent from pillar to post will remain the price of asking for justice.

Figure 7: Victims and those assisting victims who approached the police through a personal network were three times more likely to recover the full amount lost in cybercrime than those who did not contact anyone.



Note: Rest did not respond to either of the questions. All figures are in percentages. The table includes responses from both the victims and those who assisted cybercrime victims.
Question asked: Were you able to recover your lost money – yes, full amount; yes, partial amount; no? Question asked: Did you have to contact someone in your personal network to put pressure on the police to deal with your case properly?

BANKS ARE THE FIRST LINE OF DEFENCE

Better Inter-Agency Coordination Needed

India is writing a new chapter in digital finance. Since its launch in 2016, UPI has grown from 1.78 crore transactions to over 24,162 crores in FY 2025-26, worth about Rs 314 lakh crore, and now runs across 741 banks (PIB, 2026). The IMF recognises it as the world's largest real-time payment system.

But there is a worrying side to this story: Digital safety has not kept pace.

Between 2021 and 2025, the National Cybercrime Reporting Portal (NCRP) recorded more than 65.89 lakh financial fraud complaints, with reported losses of over Rs 55,050 crore. Only about Rs 8,189 crore was marked as lien, and just over 1.95 lakh FIRs were registered (I4C, NCRP & CFCFRMS data).

A single phone call. A link that looks like it came from your bank. A payment request you didn't expect. In India today, these small moments are where cybercrime begins, and they can end with a lifetime of savings gone in minutes.

Over the past decade, cybercrime has become part of everyday life in India, touching people's money, their data, and their sense of safety online. It spares no one: Anyone with a phone, a bank account, or a social media profile is at risk. What began as scattered, individual acts of fraud, has now grown into a highly organised ecosystem, with networks that operate across state lines, target victims across communities, and exploit gaps between institutions.

At the centre of this ecosystem sits one critical player, the bank. Money lost to fraud almost always travels through bank accounts, which makes banks both the first line of defence and the most important point of intervention. Yet no bank can tackle this alone. Criminals move fast across jurisdictions, while institutions often respond in silos.

This article draws on the key findings of the *Status of Policing in India Report 2026: Cybercrime—Victim Experiences and Systemic Responses* report to examine the role of banks in the fight against cybercrime, and why stronger coordination between banks, law enforcement, regulators, and other institutions is essential to stopping fraud before the money disappears.

> ***"Over half of the victims of digital financial fraud (52 per cent) reported lodging complaints independently with the bank. In contrast, four in ten of those who aided or helped a victim of cybercrime (41 per cent) reported that a complaint was filed separately with the bank"***

Complaints to the Bank

The rapid escalation of cybercrime in India has underscored the need for a systematic response mechanism, including prompt reporting of cyber fraud to banks by victims. Over half of the victims of digital financial fraud (52 per cent) reported lodging complaints independently with the bank. In contrast, four in ten of those who aided or helped a victim of cybercrime (41 per cent) reported that a complaint was filed separately with the bank. At the same time, over two-fifths of the victims (44 per cent) and close to half (47 per cent) of those who assisted the cybercrime victims did not file a separate complaint with the bank.

To understand reporting behaviour across socio-economic groups, the responses were analysed by the economic class of the victims. The data reveals a clear class-based pattern in complaint behaviour. Respondents from rich economic

backgrounds show the highest likelihood of filing complaints with banks (63 per cent), compared to other income groups. In contrast, the most economically disadvantaged (43 per cent) and those from lower income brackets (50 per cent) were less likely to complain to the bank separately.

Recovery of Money

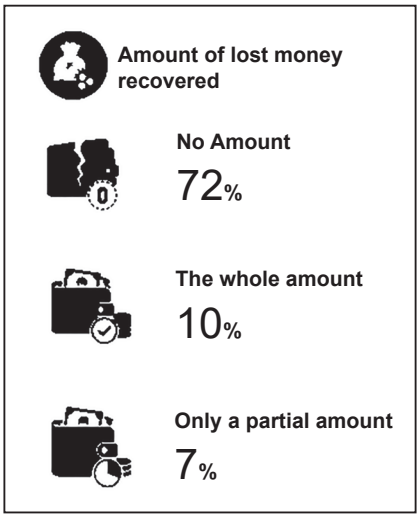
Recovering lost money is a key measure of how well cybercrime response systems work. Among victims of digital financial fraud and those who assisted them, 72 per cent reported that none of their lost money was recovered **(Figure 8)**. Only one in ten said the full amount was recovered, and 7 per cent recovered a partial amount, so just 17 per cent recovered their money fully or partially. Overall, the vast majority of victims received little or no restitution, meaning meaningful recovery was not achieved.

Victims' experiences with cyber fraud resolution are not only shaped by whether they recovered their lost money, but also by how quickly the recovery takes place. The time taken to restore funds can significantly influence victims' perceptions of the effectiveness of institutional response mechanisms. The data indicates that financial recovery, when it occurs, tends to happen relatively early for a significant proportion of victims. Nearly a third of the victims and those who assisted cybercrime victims (32 per cent) reported recovering their money within 15 days of the incident, while 17 per cent were able to recover the amount within 16 to 30 days. About a quarter (24 per cent) reported that they were able to recover their money between one to two months, and one in ten said that it took more than two months to recover their money.

Institutional Response and Effectiveness

Victims of cybercrime approach several institutions in seeking resolution, among them banks and regulators such as the RBI and the Banking Ombudsman. How they rate these institutions can differ widely, depending on the nature of their interaction and how effective the response was.

Figure 8: About three out of four victims and those who assisted them could not recover any of their lost money



Banks are often the first point of contact, yet their performance receives mixed reviews. On their role in recovering lost money, 32 per cent of digital financial fraud victims and those who assisted them were satisfied (11 per cent very satisfied, 21 per cent somewhat satisfied), while 38 per cent were dissatisfied (16 per cent somewhat dissatisfied, 22 per cent very dissatisfied). Notably, one in four (24 per cent) said they never used this service.

Regarding the RBI Banking Lokpal mechanism, a little over a quarter of respondents (27 per cent) were satisfied (9 per cent "very satisfied", 18 per cent "somewhat satisfied"), while one in five (20 per cent, combining "somewhat" and "very dissatisfied") were dissatisfied. A striking 46 per cent said they had never used the Lokpal services. One possible reason is limited awareness among victims that the RBI Banking Lokpal mechanism exists.

Bank-Police Coordination and Victim Satisfaction

Coordination between banks and the police is central to complaint redressal in financial cybercrime. Although systems such as the Indian Cyber Crime Coordination Centre (I4C) are meant to ensure seamless coordination, significant gaps remain in practice, making redressal harder for victims. The survey

reflects this, with many victims and those who assisted them reporting low satisfaction.

Figure 9 shows mixed satisfaction in both groups. While 11 per cent of victims were "very satisfied," the share fell by nearly half, to 6 per cent, among those who assisted victims, though overall satisfaction was similar (37 per cent and 35 per cent). Meanwhile, 20 per cent of victims and 22 per cent of those who assisted were "very dissatisfied", and 16 per cent and 17 per cent respectively were "somewhat dissatisfied." Over one in ten respondents in both groups said there had been no coordination between the bank and the police.

Satisfaction also varied with the recovery of money. Among those who recovered the full amount, 49 per cent were "very satisfied", 43 per cent were "somewhat satisfied", and none were "very dissatisfied". Those with only partial recovery reported more mixed experiences: Just under one in five (17 per cent) were "very satisfied", while more than half (54 per cent) reported being "somewhat satisfied", with a small share expressing dissatisfaction (20 per cent – 7 per cent "very dissatisfied" and 13 per cent "somewhat dissatisfied").

Conclusion

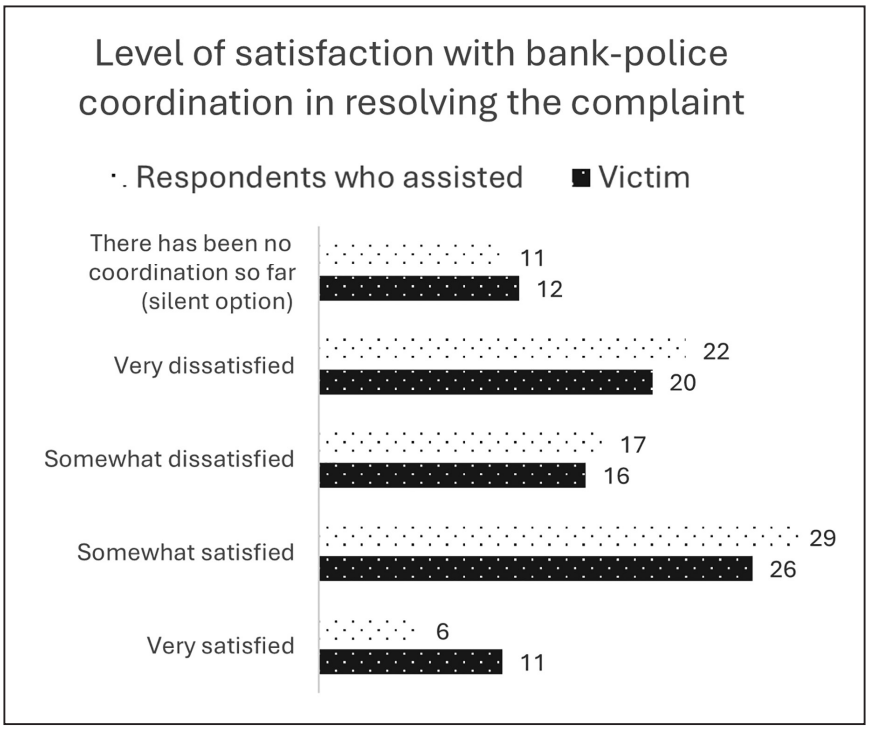
This article examined how banks and regulatory institutions respond to cybercrime victims and how satisfied victims are with that response. The findings show a banking system that is only partially functional, accessible to some, and uneven in its effectiveness.

Although many victims engaged with their banks and lodged complaints, this did not translate into meaningful recovery. Nearly two-thirds reported the fraud within 24 hours, and nearly half had their bank accounts frozen after complaining. Yet a vast majority recovered nothing, and recovery was slow for those who did, except for a third who recovered their money within 15 days. Wealthier and rural victims were more likely to complain to banks.

Satisfaction with the bank's role in recovering money and with the RBI Banking Lokpal is tepid, with around three in ten satisfied and a similar share dissatisfied. A significant share never sought the bank's help in recovering money (24 per cent), and an even larger share never accessed the RBI Lokpal (46 per cent). Victims whose money was fully recovered were more likely to be satisfied with the bank's role.

Seamless bank-police coordination is also essential to effective resolution. About a third of both victims and those who assisted them were satisfied with this coordination, though a slightly higher proportion were dissatisfied.

Figure 9: One in five victims of digital financial frauds are very dissatisfied with the bank-police coordination in their case



CYBERCRIMES: VICTIMS, RESPONSES, ACCOUNTABILITY

Excerpts From A Panel Discussion



Panellists Launching the Status of Policing in India Report (SPIR) 2026 at New Delhi

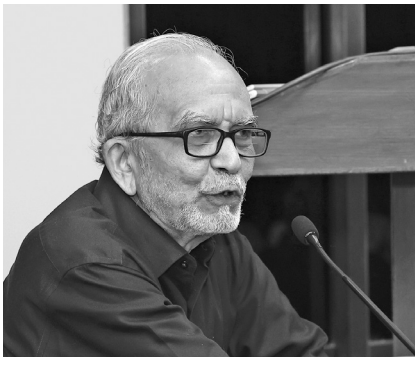
The Status of Policing in India Report (SPIR) 2026, jointly produced by Common Cause and Lokniti–CSDS, was launched on September 24, 2026. The report focuses on "Cybercrime: Victims' Perspectives and Systemic Responses", based on a 16-State survey of 8,306 citizens mapping cybercrime exposure, vulnerability patterns, and police redressal mechanisms.

A panel discussion was held during the launch at India International Centre, New Delhi, which saw the participation of eminent speakers from varied fields.

Excerpts:

Prof Suhas Palshikar, Social Scientist, Author and Columnist:

While this is a report on status of policing with respect to cybercrimes, earlier we have already



done a report on surveillance. In the sense, the intrusion of the digital into our lives has already been noticed, noted and commented upon and experienced too. This report, in a sense, touches upon a one slice of the reality, namely cybercrimes. But the question this report might leave us with is, whether cybercrimes also happen because of the overall culture of surveillance and the fascination with surveillance technologies. At the same time, whether there is a religion called the digital and our faith in that religion is so much that we believe that whatever is digital is secure without necessarily going into the actual security

credentials of any gadget or any service. These would be nagging questions.

The other nagging question this report probably leaves inadequately answered and that is not for want of our wish to do it, but for want of the ability to access and get information on various non-financial aspects and methods of cybercrime.

And the third, which comes out repeatedly in the report, is about this deep social divide which we come across every time when we talk of policing. And by policing I am not talking only of the police here, because this report also takes one step further by expanding the idea of policing—whoever is in charge of the function of protection—and thus, banks come into the purview. The social divide is whenever you come across any victim, you first find out who the victim is and by identifying the victim you decide whether you attend to the victim diligently, over-efficiently, casually or carelessly. It is this social divide which comes across all reports on policing so far.

Mr Sanjay Sahay, IPS (Retd.) and Cybersecurity Expert

Cybercrime is a huge gamut of stuff which is primarily happening at an industrial scale. The whole thing starts in the backdrop of a very loose data regimen, and that data regimen is not at all restricted to the government itself. [It is]



Because we are desperate to put our data in the public domain. And when that data is there in the public domain, there are people who can harness the data.

Talking about social engineering: How does social engineering come into existence? There is a whole bunch of data which is thrown at you so that you believe that I'm aware of everything and I am in a position by which I can give you some benefits. The biggest challenging part is, why do people who are not a part of any criminal activity, accept this? This is primarily because of the manner in which we hold public authority in this country – primarily fear and complete distrust. From there, everything starts and Indian policing and Indian governance remains a matter of perception rather than a matter of delivering.

Now, the issue of investigation. How can investigation happen? Ninety-seven per cent of the top 500 companies have been hacked, and the other three per cent are not aware that they have been hacked. The most popular password 10-15 years back was 1 2 3 4 5 6 7, and today also it remains the same. That is where we are, and that is the way the Indian police works, where you find passwords on notice boards. That is their capability of keeping their system safe.

We come to the registration of the case. Sixty-five lakh complaints landed to I4C, of which nearly two lakhs have been translated into FIRs. So, what is the total quantum of police you will require? It should be at least as much as the conventional police. Second, what the expertise of that particular imaginary cyber police should be in comparison to the current police? You go to any police station in this country, cyber police in the country, you'll rarely find a fellow who understands anything of cyber forensics. That's the reality of life.

This whole issue is [further] complicated by the fact that there is zero ownership and zero responsibility. How can any institution in a democratic country have the audacity to decide to register or not register, investigate or not investigate, communicate or not communicate? They behave in a manner which would, I think, put even a monarchist to shame. Who is primarily responsible for cyber security or cybercrime? Here, only the victim is [held] responsible. That is what the government is telling you.

We are not able to take care of the data which is splashed all around the place. We don't have

anything which we can call as the deep web or the dark web police. However much we talk about AI, I don't think there is anybody who is working with AI and cyber-crimes.

Now the investigation part of it—we have not gone beyond the cases getting charged-sheeted. The first case which got conviction in Karnataka – when we had a [cyber] police station since 2001 or 2002 – was only in 2013–2014.

Now, in this whole gamut of things, one [question] is whether without expertise we can run the show? And second, who has the expertise? These are questions which I leave open. Suffice to say that we are living in a real-time dynamic world. Cybercrimes happen in that manner and any response to it has to be in real time and dynamic.

There are 1.8 million mule accounts. There is no database of mule accounts which is given to us.

One simple thing they can start with is whitelisting of government phone numbers. So, it [is displayed] as a government phone number. Anything which is outside of that, we need not bother. There's an industrial scale infrastructure which is happening from here to Southeast Asia, from cryptocurrency to variety of other things, and that is what propels the whole thing. Yet, the government has not gained the capability to match something of this nature.

Dr Ranjana Kumari, Director, Centre for Social Research



As a whole generation of people, we are living in a very different time. The reason why we all are very worried about cyber security and cybercrime [is] because it is no more general Artificial Intelligence; it is moving into quantum and then, of course, into super intelligence.

A lot of other countries have e-safety commissions. Have we ever thought of that? We do need to have institutional mechanism, trained personnel and also people who believe in changing the systems.

Policing in our system has a basic [limitation]. The total system is constructed and built upon post-harm response. When the crime happens, then you bring in the police, you bring in the law, you bring in the judiciary. They [the perpetrators] are much, far ahead, much more sophisticated than our systems are.

We deal with cases of non-consensual posting of images. In that situation you don't even realise, you don't even know; it moves very fast. It multiplies on various platforms. Hashes are not very easy to control. Even [though] the cyber police [is] trying its best to support, it's very difficult. What we need [is] a new modern institution which looks at what cybercrime is all about? I4C is there but with a police perspective. They try to do whatever they can in a very limited way. We get lots of reports of women who come and say that post-divorce husbands are is threatening to post intimate images; post friendship young girls come and say that "look my life will be over. I'm going to commit suicide if this is posted." This is the socio-psychological impact.

So, let me just come to some issues which I feel immediately need to be paid attention to. Identify a separate agency. It cannot be just home ministry, MeitY, etc. Develop a whole new e-safety commission which is going to ensure that systems are put in place. Globally, countries have it now.

A whole unprepared society [is being] pushed into a digital arena. Everybody has a phone, everybody has internet. But how much have we prepared our people? What is the messaging? Are we telling our children how to protect themselves? Who are the predators online? How do children protect themselves while playing games; if somebody enters that game and starts asking for nude photos? We have found in our

research that even very young children are posting their nude photos online. So, [we need to] pay attention to awareness-building among the people.

We don't just start asking for institutions to train. Of course, that's the most urgent thing the government should respond to at the moment. But also, from the people's side, we need to build education system around digital [use]. We have to start bringing in the courses [right from] from childhood.

All this [cybercrime] is happening much more to women and children. Women are being seriously victimised and they are not reporting. Women don't even walk into the police station. Even the most educated and smart ones are not doing it. We should collectively start putting pressure on the systems which should respond to our work.

Mr Saikat Datta, CEO and Co-Founder, DeepStrat

In my view, we are all looking at it [cybercrime] [in a] very piecemeal [manner] without understanding what are the fundamental issues [because of which] cybercrime today has become so pervasive.

The problem with policing is we look at it as a monolith, without realising that in the Indian constitutional scheme of things, law and order is a State subject. It's very easy to say I4C is doing



this and that, but I4C is a central body. It cannot go into the states and address the issues, and nor should it [do so]. Because when a crime takes place in a state, the primary responsibility is of that state. Therefore, what you do at the state level is more important than what we are trying to do at the central level. But because the Centre has more finances, the states end up almost struggling for resources, when they are best placed to actually address that issue.

The second problem is our policemen; think of the constabulary. Whichever states you come from, if you are from a southern states like Telangana, Andhra, Karnataka, Kerala, think of the average policemen you interact with. Then think of the states of say, Haryana, UP or maybe Bihar and think of the local constable, and you can draw your own conclusions on what is your perception is. A lot of this perception is also driven by the level of training, culture, etc., that decides how policing is being done in those states vis-à-vis the southern states.

There is a very stark cultural issue. If I were to go to a state like Kerala, Telangana or Karnataka, the average constable constabulary is far better educated and far better placed. When there is a huge cultural difference for a series of reasons, the response to a technologically-aided crime like cybercrimes becomes very different. When we worked in Haryana, we saw the struggle they have because nobody is aiding them. There is no dedicated training, there is no dedicated orientation for helping the police to deal with cybercrimes. Expecting them to take a deluge of cases and then deal with it is very unrealistic.

In 2020, just after the first lockdown was over, we did a cybercrime study. At that time, Gurgaon had only one police station dedicated to cybercrime, and in that one police station, which was handling entire southern Haryana, there were only about 1,200 complaints [over 10-11 months]. Today, they are getting about 1,500 to 1,600 complaints every day. That's the scale. The amount of money that was defrauded from the State was close to about {Rs] 800 crores in just eight months. If you then start thinking of recovery, where and how do you begin?

Burking is where the police ensure that no FIR is lodged. Because every police station does wants to maintain a record that crime is low in their jurisdiction. Why is burking a cultural issue?

Because there is no capacity in policing today to deal with the deluge of complaints that come their way in various sections of the law.

The next problem is technology, and there is a technology asymmetry globally. Countries which have emerged out of colonialism like India, because of lack of resources and many other issues, we have not been able to keep up with technology, whereas the Western world has moved far ahead.

When it comes to cybercrimes, there is a lack of understanding of how the technology works. Many times the technology and the understanding can come through collaboration and cooperation with some of the technology firms and the Indian law enforcement. The problem is, if the tech companies who understand the technology [and] can collaborate, if they are scared to talk to the police, then where does the collaboration actually start? This is a foundational problem. As a result, there is no collaboration. We want to have a whole of society approach but the whole of society will never happen when parts of the society are in conflict with each other.

When you don't have a whole of society approach, then you are also dealing with another very important challenge, of digital arrest. Mr Nandkumar Sarvade says, the core reason why we are falling prey to digital arrest today is because of our fear of authority. Even very well-off people will immediately fall prey to it. The fear of authority is then weaponised by the scamster. Unless those issues are addressed, cybercrimes will continue to grow exponentially.

Lastly, definitional clarity is very critical. Our understanding of cybercrime is actually not the global understanding of cybercrime and it is also piecemeal. We don't look at cyber-security related issues as cybercrimes; we look at it separately. Our understanding of cybercrime is driven mostly as a retail financial services crime.

Today, AI is again changing the way cybercrimes are taking place. Fact of the matter is, technology was already far ahead, and it's gone to another dimension. Our policemen, who are used to not dealing with even normal everyday crimes, how will you expect them to tackle something at that level? And because our states are not being given adequate funds, training programs, etc., we are never going to get out of this problem.

Mr Nikhil Pahwa, Digital Rights Activist, Founder of Medianama

Let me first start with what my SIR data reveals about me. So, someone sent me an email at the beginning of this month pointing me to a website that he had built. So, I went to that website and put in my own name to see



what it reveals. It was able to identify on the basis of my location, my name and the people in the same district as me – who my relatives might be, including generational relationships; who my neighbours are, based on the address of the information and the [people] in my neighbourhood who are on the voters' list. It creates a relationship graph around each person and that actually is what is at the core of social engineering and our governments have very helpfully released a truckload of this information historically over time.

For example, when we were reporting on Aadhaar in 2013-14, entire government departments had put up spreadsheets of person's name, addresses, mother's name, date of birth, phone number and everything that you might need to open a bank account. In some cases in Andhra Pradesh at that time, there were even school children's data that was available. As we start connecting people to a unique ID, we've done very little to protect it. You've allowed accumulation of data, you've

allowed interconnection of that data, which is leading to an information asymmetry between the victim and the perpetrators.

Using AI, someone can mimic the voice of a person because the voice could be cloned from other phone calls. Voice cloning is becoming very easy now and it's not very expensive to do. So, what you're seeing is a relationship graph with real-time information on you because of either what you have put [up] on social media or what other databases might reveal about you, which may already be leaked.

Alongside that, you have people who have industrialised social engineering. I remember almost five years ago, Snigdha Poonam had done a story about Nuh in Haryana, where entire call center operations were running. They had daily targets, monthly appraisals, and an annual party where awards were given to the biggest scamsters. They were buying SIM cards by the bulk.

Digital makes things easier for us. It is meant to reduce friction in what we do. As you keep reducing friction, you become, as Nand Nilekani calls it, a data-rich country. This entire system also forms the basis of the fraud that we are seeing today. It's impossible to address this fraud without dismantling organised crime.

Aadhar is the fountain head of social engineering and fraud and it's not something that we hadn't warned against. I would go as far as saying that Aadhaar is actually a national security problem. That data is already on the dark web. If you remember, Rachna Khera had reported that Aadhaar database was being sold by employees of common service centers for 800 rupees. Fraud mule accounts [are] very easy to set up.

It's easy to blame the banks. But banks themselves don't know how to deal with the situation. Instead of becoming more convenient, bank apps are becoming increasingly more inconvenient because they're trying to fight fraud.

The police are also struggling to deal with this. At the core of it lies the fact that we are constantly releasing data about ourselves, not [always] through our own consent, but also by the government. The government is actually responsible for the scale of cyber fraud happening in this country. They have built the infrastructure for fraud in this country because of how much data it leaks out and they have no intention of stepping back because, as we all know, that also is a foundation of the surveillance infrastructure in the country.

Government bodies are largely exempt from the data protection law in this country. We should never forget that the Government of India went to the Supreme Court arguing that privacy is not a fundamental right. The data protection law that we have is built in order to exempt the government, but also to treat privacy as not a fundamental right.

The government is building system upon system trying to make things more difficult for us with the objective of tackling cybercrime, because they've already created a mess that they cannot solve. They're now trying to create more hindrances for citizens. For example, you have facial recognition when you're buying a SIM card. How do you know how secure that data is when they're taking your facial data, that can be used to create AI clones of people?

We can keep holding platforms accountable for what they're doing, but we should also recognise that a large part of our freedoms is being regulated by the government through the platforms. So, while we want certain harmful content to be censored, also remember it's nearly impossible for any platform to effectively police a billion people online. The restrictions that we create for safety, those restrictions can also be weaponised for censorship. We should be careful about what we wish for.

COMMON CAUSE EVENTS

Prakash Singh v UOI: 20 Years of Police Reforms

Sept 22, 2026, New Delhi: To mark the 20th anniversary of the landmark *Prakash Singh vs Union of India* judgment, the India International Centre organised a discussion on Police Reforms. Those who participated were Mr Prakash Singh, former DGP of UP, BSF, and Assam, Mr G K Pillai, former Home Secretary of India and retired Supreme Court judge, and Justice Vineet Saran, who also chaired the meeting. Common Cause director, Dr Vipul Mudgal, moderated the discussion. He also expressed his views, along with IIC Director, Mr K N Shrivastava, IAS (Retd). Common Cause was also one of the co-petitioners in the landmark case.

Article Contributed to an Edited Public Policy Book

September 2026: Radhika Jha, Project Lead, *Rule of Law,* and Dr Vipul Mudgal, Director, Common Cause, contributed to an edited volume titled *Policy Analysis in India,* edited by Azad Singh Bali and Satyajit Singh. The chapter, titled 'Mapping institutional deficiencies in India's criminal justice system as instruments of policy analysis', examines patterns of policing across India and draws heavily from the Status of Policing in India Report series.

Published by Bristol University Press, the volume is part of the International Library of Policy Analysis Series and is available here: https://policy.bristoluniversitypress.co.uk/policy-analysis-in-india.

A Discussion on Delhi Police and Citizenry

On August 6, 2026, the Press Club of India organised a panel discussion on Delhi Police and Citizenry in the aftermath of the brutal police action against the youth protesters of the Cockroach Janata Party (CJP). The speakers included Common Cause Director, Dr Vipul Mudgal; retired IPS officer, Mr Yashovardhan Azad; Editor of *The Wire*, Ms Seema Chisti; student leader, Ms Neha Bora; and a pellet gunshot victim, Mr Irshad Mansoor. The discussion was moderated by the Press Club of India President, Ms Sangeeta Borooah Pisharoty.

Webinar on Accessibility as Common Cause: The role of PILs in seeking Justice

On July 31, 2026, IIT-Madras organised an online lecture by Common Cause director, as part of the Accessibility Research Centre (ARC) Webinar Series, *Accessibility Without Boundaries (AWB)*. The series was aimed at fostering a dialogue on inclusive practices across education and public life. Dr Mudgal addressed a well-attended interactive session with students and faculty members from various disciplines of the institution, and Ms Divya Chauhan, Legal Officer, Common Cause, facilitated a Q&A session at the end of the event.



Audience at the Launch of the SPIR 2026

DIGITAL HYGIENE AND SECURITY HABITS

How We Pay and Protect Ourselves Online?

This piece condenses Chapters 7 and 8 of the Status of Policing in India Report 2026 (published by Common Cause and Lokniti-CSDS), which draws on face-to-face surveys of 8,306 respondents, conducted in 16 states and one UT across India. Chapter 7 maps how Indians pay online and how safe they feel doing so; Chapter 8 examines what they actually do to protect themselves. Read together, they describe a country that has adopted digital finance faster than it has learned to secure it.

India's digital payment habit has outrun its security habits. Almost half of respondents use UPI every day. Yet one in five does not use two-step verification, and the respondents most prone to risky behaviour are the most likely to call online banking very safe.

Table 3: Frequency of use of different digital financial services

Usage of	Frequency of use			
	Daily	Once or twice a week	Once or twice a month	Never
UPI	49	24	8	17
Mobile Banking apps/net-banking websites	32	25	15	34
Online investment or other financial services (FDs, mutual funds, stock trading, etc.)	9	18	13	55
Digital Loan apps (LazyPay, Money Tap, etc.)	5	11	12	66

Note: All figures are in percentages. The rest did not respond.
Question asked: How often do you use the following – daily, once or twice a week, once or twice a month, or never?

A country that Pays by Phone

Digital payments have become deeply embedded in everyday financial transactions. UPI is by far the most widely used digital payment mode. Almost half of respondents (49 per cent) use a UPI app daily and another quarter (24 per cent) weekly; only 17 per cent have never used one. Mobile banking apps and net-banking sites are used daily by just 22 per cent, and a third (34 per cent) have never used them. Specialised products remain a minority pursuit: 55 per cent have never used online investment services, and two in three (66 per cent) have never tried a digital loan app (Table 3).

The advantages of this digital expansion are however not equally distributed. Men, urban residents and the affluent are the heaviest users of online payments: 31 per cent of men are high users against 21 per cent of women; 29 per cent of urban respondents against 18 per cent of rural ones; and 42 per cent of the richest against 16 per cent of the poorest.

The Confidence Trap

UPI was rated as the safest payment channel by the respondents, with over a third of the respondents (34 per cent) finding it "very safe", and another two in five (41 per cent) reporting it

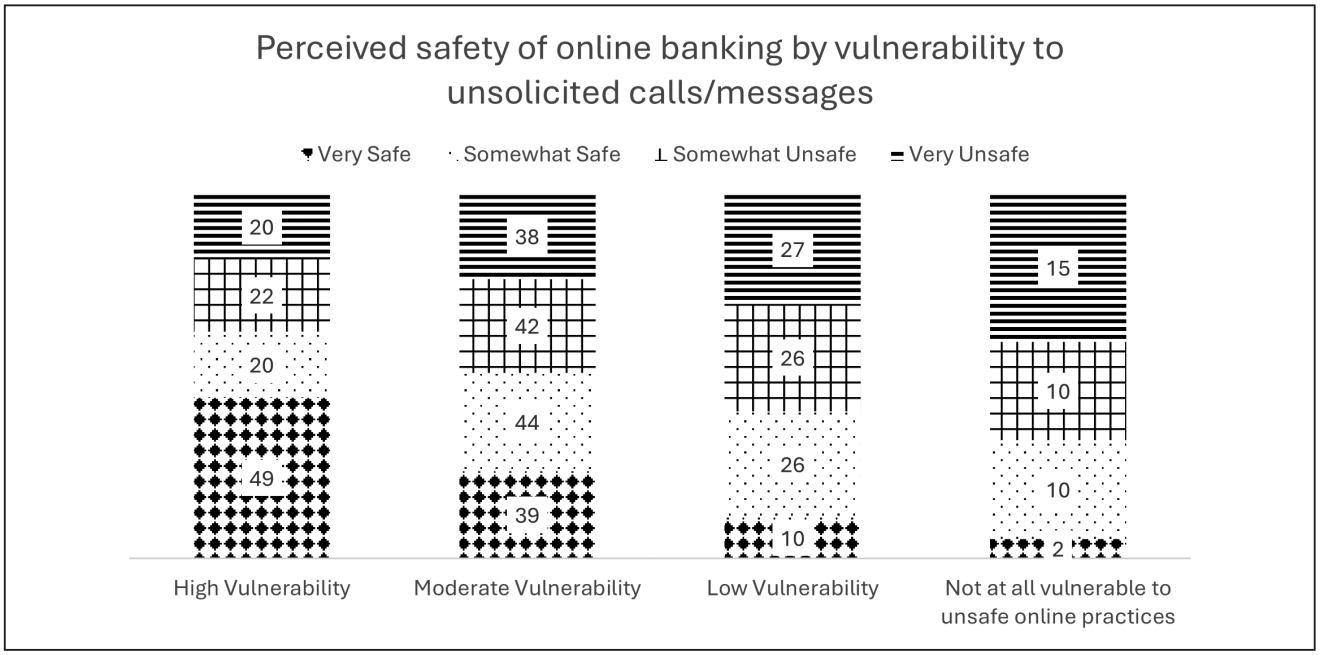
to be "somewhat safe", bringing the combined positive perception to about three-fourths of the respondents – 75 per cent. The combined proportions of debit and credit cards (65 per cent), wallet apps (64 per cent), mobile banking apps (60 per cent) and internet banking sites (50 per cent) rank below it. Digital loan apps and stock-trading platforms inspire far less confidence: Only 8 per cent rate each very safe, while 47 per cent and 46 per cent respectively consider them unsafe. Taking the five mainstream modes together, 63 per cent of respondents consider online banking safe (23 per cent very safe, 40 per cent somewhat safe) and 37 per cent consider it unsafe.

Victimisation is higher among the most active and most confident users. Of respondents who use UPI many times, 16 per cent reported being victims of cybercrime in the previous two to three years, against 7 per cent of non-users; the report links this to greater exposure, and finds that use of other payment modes makes little difference. Among respondents who rate online banking very safe, 28 per cent were victims or close aides of victims, twice the 14 per cent among those who rate it very unsafe.

It is important to note how usage breeds trust: The most used modes and apps are the most trusted, while loan apps and trading platforms are used little and viewed with scepticism. This trust also extends to telecom providers, which sit at the centre of many frauds: 74 per cent of respondents trust their provider a lot (26 per cent) or somewhat (48 per cent) to keep their number and personal information safe, which the report reads as a notable sign of public confidence.

While most respondents report cautious behaviour when dealing with unknown callers and messages: 68 per cent say they never share an OTP or press a button when asked to do so, while 56 per cent never click unknown links or open unknown files. A sizeable minority engages in such behaviour at least sometimes, with 14 per cent sharing OTPs and 21 per cent

Figure 10: Perceived safety of online banking by vulnerability to unsolicited calls/messages



Note: All figures are in percentages.
Question asked: If you receive any of the following from an unknown person or number, will you do the following: a) Click on a link that you received c) Open a photo, video or other type of file d) Press a button or number if an unknown caller asks you to do that e) Share an OTP with the caller – yes, mostly; yes, sometimes; or never?
Question asked: In your opinion, how safe are these modes of online banking: a) UPI b) Mobile banking apps c) Internet banking websites d) Debit/credit card payments g) Wallet-based apps – very safe, somewhat safe, somewhat unsafe, or very unsafe?

pressing a button. On the report's vulnerability index, 10 per cent of respondents are highly vulnerable to unsolicited calls and texts, while 23 per cent are moderately vulnerable.

Paradoxically, respondents who are most likely to click unknown links, open unfamiliar files, follow a stranger's instructions or share an OTP are also more likely to consider online banking very safe. Nearly half (49 per cent) of the most vulnerable group rate online banking as very safe, compared with about 20 per cent of the least vulnerable (Figure 10). The report identifies this combination of low vigilance and high confidence as a potential risk factor for cybercrime, highlighting the need for awareness campaigns that foster a more realistic understanding of online threats.

The Safeguards People Use

Chapter 8 examines the practical steps respondents take to protect themselves. Two-step verification, which requires users to complete an additional authentication step, is one of the basic safeguards available for digital financial transactions. Yet, its use remains far from universal.

Among respondents, 55 per cent report using two-step verification on UPI apps, compared with 38 per cent on internet banking apps. One in five (20 per cent) does not use it for UPI transactions, while 12 per cent are unaware of the facility. For internet banking, 26 per cent do not use two-step verification and 16 per cent do not know about it.

The differences in adoption follow familiar patterns of digital inequality. Among respondents below the age of 25, 68 per cent use two-step verification on UPI apps. Among those aged 56 and above, the figure falls to 31 per cent. Lower usage of UPI among older respondents partly explains this gap: One in five people in the oldest age group do not use UPI at all, compared with 4 per cent of the youngest respondents.

Education is another important dividing line. While 71 per cent of college graduates use two-step verification on UPI apps, the figure falls to 26 per cent among respondents who are non-literate. Urban respondents are somewhat more likely than rural respondents to use the safeguard (57 per cent compared with 48 per cent). The gap between the richest and poorest is wider, at 68 per cent and 43 per cent, respectively.

These disparities reveal how differences in access and familiarity can carry over into security practices. People who have had fewer opportunities to use digital financial services are also less likely to use the safeguards available within them. Awareness of a security feature, access to it and the ability to use it confidently are distinct requirements, and each needs attention.

The findings also caution against treating the adoption of a particular safeguard as a complete measure of digital safety. Two-step verification can strengthen account security, but users continue to encounter risks through unsolicited calls, fraudulent links, misleading websites and requests for personal information. Protection depends on a combination of technical safeguards and everyday decisions.

Awareness Without Everyday Habit

Cybersecurity awareness campaigns have reached a large proportion of respondents. Some 45 per cent of respondents have both received a cybersecurity message and seen an advertisement, 21 per cent have only received a message and 22 per cent have only seen an advertisement; just 7 per cent have seen neither (Figure 11).

However, exposure to these messages has not translated into routine practice. Receiving a warning about cybercrime does not automatically translate into checking an app's permissions, avoiding password reuse or verifying the authenticity of a website before entering personal details.

The report's digital hygiene index examines several such practices, including avoiding public Wi-Fi, not saving passwords in browsers, checking app permissions, avoiding password reuse and verifying website or app authenticity. The findings show that secure habits

are far from routine for many respondents. Across these practices, roughly a quarter report always following the recommended precautions, while similar or larger proportions say they never follow them.

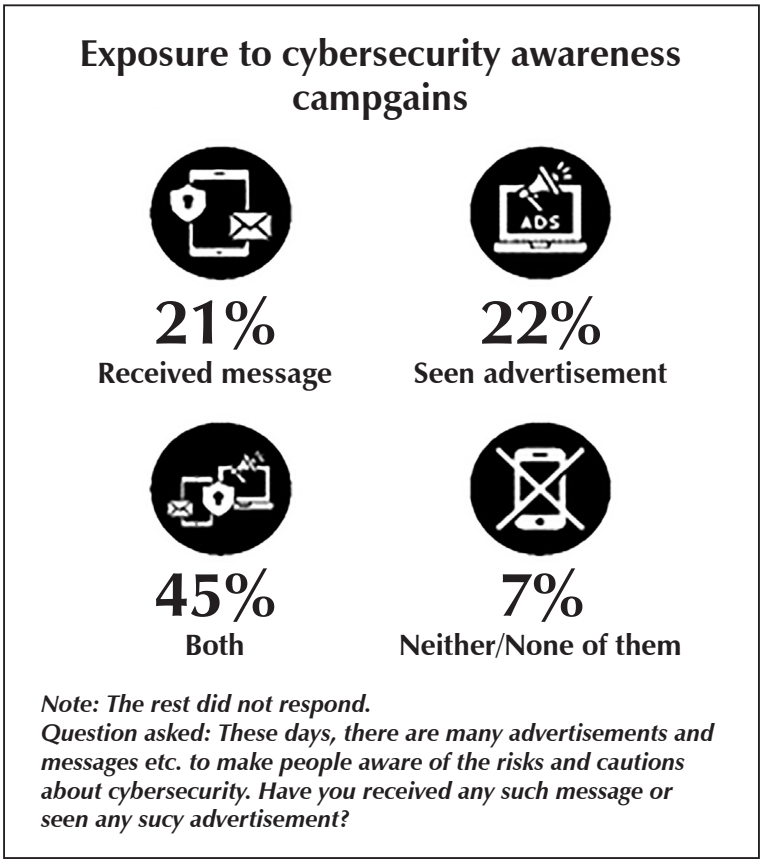
For instance, 27 per cent always avoid using public Wi-Fi, while 27 per cent never do so. A quarter (25 per cent) always check app permissions, but 29 per cent never do so. Nearly a third (29 per cent) never avoid reusing passwords, and 31 per cent never verify the authenticity of a website or app.

Awareness is an important starting point, but the report shows that it cannot be treated as evidence that these habits have taken hold.

Digital hygiene also varies by age, education and location. A quarter (25 per cent) of respondents below the age of 25 always follow secure practices, compared with 15 per cent of those aged 56 and above. Among the oldest respondents, 36 per cent never follow such practices. The proportion who always follow them rises from 15 per cent among non-literate respondents to 27 per cent among graduates. Urban respondents are also more likely than rural respondents to report always following secure practices; at 22 per cent and 17 per cent, respectively.

These differences mirror the inequalities observed in the use of digital financial services and two-step verification. Digital safety depends partly on whether people have the knowledge, confidence and opportunity to make informed choices. Campaigns that rely on written messages or general warnings may have limited value for users who need practical guidance on how to recognise a scam or change a security setting.

Figure 11: Exposure to cybersecurity awareness messages and advertisements



Closing the Digital Literacy Gap

The two chapters describe a system that has scaled faster than its safeguards. The groups least integrated into digital finance, including women, the poor, rural residents and older users, are less likely to use basic protections, and the most confident users are the likeliest to be victimised. The report concludes that digital financial inclusion should be paired with targeted literacy programmes for women, older users and lower-income groups, who use digital finance less but are not necessarily less exposed to its risks, and that awareness campaigns should teach practical skills, risk awareness and safer behaviour.

TRUST AND VULNERABILITY ONLINE

How Competent Are Our Institutions?

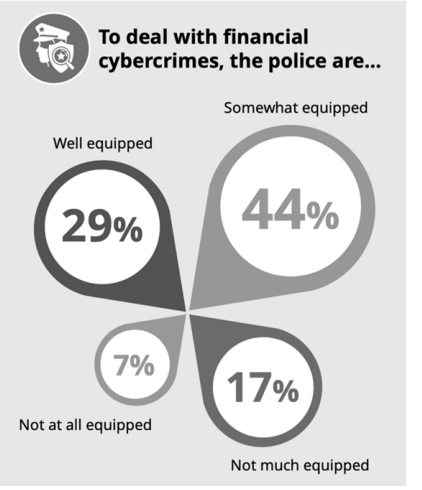
Chapter 9 of the SPIR 2026 unpacks vulnerabilities in digital trust, security, and privacy, while also identifying opportunities to strengthen the digital ecosystem. Easier digital transactions and other online financial services have empowered people. But it comes with routine encounters with scams, identity theft and privacy violations.

In such a context, effective redressal mechanisms have become essential. India has developed a range of institutional systems to address cybercrime, and these have expanded over time. It includes Indian Computer Emergency Response (CERT-In), Indian Cyber Crime Coordination Centre (I4C), National Cybercrime Reporting Portal (NCRP), and Cyber Crime Prevention against Women and Children (CCPWC) scheme. These bodies act on a spectrum of monitoring cybercrimes, co-ordinating amongst different agencies and providing funds for capacity-building and training of the personnel.

However, an important question is: Are these systems truly accessible and effective in practice? Cybercrime redressal mechanisms involve different stakeholders, including police, bank officials, judges and magistrates. While these mechanisms offer formal accessibility via helplines, portals, complaint registration processes and investigations, data shows that their functioning is uneven. Issues such as procedural complexities, significant delays, failures in timely account freezing, limited financial recovery, and, in some cases, reliance on personal networks to exert pressure on authorities continue to affect perceptions. Although the government aims to strengthen coordination through various mechanisms and address these gaps, only a small proportion of such cases reach courts, and even fewer are resolved. Such a condition reflects a clear gap between formal access to the redressal mechanism and citizens' actual experience, which ends up shaping public evaluation of these institutions.

Against this background, we aimed to analyse public perceptions of the police, banks and courts and to assess whether they are perceived as capable enough to fight cybercrimes. In a similar vein, we examined the likelihood of citizens reporting cybercrime in the future. Also, how people assign responsibility for data protection – whether they view it as primarily the responsibility of individuals, or of governments and banks. Lastly, it seeks to understand what citizens expect from the government when it comes to ensuring digital safety in a risk-prone digital environment.

Figure 12: Nearly three out of four people feel that the police are equipped to deal with financial cybercrimes.



Note: All the figures are in percentages. The rest did not respond. Question asked: In your opinion, how equipped do you think the police is to deal with financial cybercrimes- very equipped, somewhat equipped, not much equipped, or not all equipped?

Institutional Capacity

The respondents were asked about their perceptions of how well equipped they think the police are to deal with financial cybercrimes. Overall, nearly three quarters (73 per cent) perceived the police to be either

very well or somewhat equipped to handle financial cybercrimes. While over four in every ten (44 per cent) thought police are 'somewhat equipped', less than three in every ten (29 per cent) considered them very well equipped (Figure 12). On the other hand, about a quarter (24 per cent) reported that the police are not equipped to deal with financial cybercrimes Seventeen per cent said that the police are "not much equipped" and 7 per cent said they are "not at all equipped".

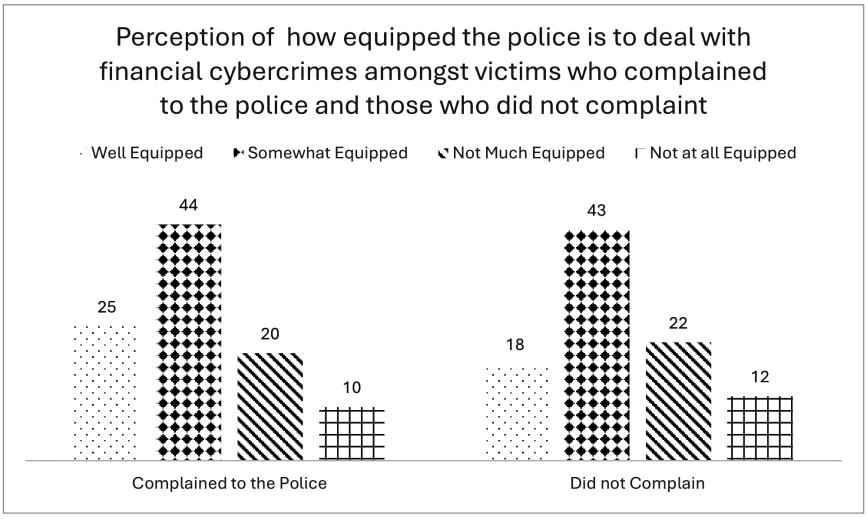
We analysed and compared the perceptions of victims and those who aided the victim against the perceptions of those who were not victims of cybercrimes. It was found that victims were slightly less likely to believe that the police are well equipped to deal with cybercrimes. While 31 per cent of the respondents who were not victims of cybercrimes said that the police are well equipped to deal with financial cybercrimes, the proportion drops to 23 per cent amongst those who have been victims of cybercrimes or have aided the victims of cybercrimes. Simultaneously, victims and those who assisted cybercrime victims are relatively more likely to perceive that the police are not much equipped (21 per cent versus 15 per ent) and not at all equipped (10 per cent versus 6 per cent) to deal with financial cybercrimes compared to non-victims.

As seen above, victims are relatively less likely to believe that the police are well equipped to deal with financial cybercrimes. However, among the victims, those who complained to the police are slightly more likely to believe that the police are well equipped to deal with financial cybercrimes, compared to those who did not do so (Figure 13). This indicates that while the overall perceptions regarding police capacity to deal with cybercrimes is not very positive amongst the victims, there is a higher likelihood for those who engage with the police to have a more positive opinion about their capacity to deal with financial cybercrimes. However, the difference in these opinions is only marginal, and not very sharp.

Amongst those who complained to the police, a quarter of the respondents (25 per cent) were likely to report that the police are "well equipped", compared to nearly one in five (18 per cent) among those who did not complain. Conversely, the perception that the police are "not at all equipped" is marginally higher among those who did not complain (12 per cent), compared to those who complained to the police (10 per cent) (Figure 13). These findings suggest that first-hand experience with police tends to have a slightly more favourable assessment of their competence.

Since bank officials, judges and magistrates, along with police personnel, have a role in the cybersecurity ecosystem, the

Figure 13: Cybercrime victims who complained to the police are more likely to believe that police are well equipped to deal with financial cybercrimes



Note: All figures in percentages. The data includes perceptions of both the victims and respondents who assisted cybercrime victims.
Question asked: In your opinion, how equipped do you think the police is to deal with financial cybercrimes – very equipped, somewhat equipped, not much equipped, or not at all equipped?

respondents were asked about their perceptions of whether the police, banks, and judges/ magistrates are trained to deal with cybercrimes. Over seven in ten respondents (72 per cent) report that the police are well-trained (combining 'very much' 36 per cent and 'somewhat' 36 Per cent).

At the broader level, perceptions about the police show a clear divide among the victims (including respondents who assisted victims) and non-victims. Non-victims (38 per cent) hold a more favourable view of the police than the victims (28 per cent), with a greater proportion citing them as "very well trained". Victims (12 per cent), in turn, are relatively more likely to report that police are "not at all trained" to deal with cybercrime than the non-victims (8 per cent).

This pattern becomes more nuanced when the victims or those who assisted cybercrime victims are further disaggregated by whether they filed a complaint. Among those victims who complained to the police about the cybercrime, about one- third (32 per cent) reported that the police are very much trained', as compared to about a quarter (22 per cent) who did not complain. While cybercrime victimisation appears to lower confidence in the police's ability to deal with cybercrime relative to non-victims, engagement through complaint appears to partially restore it.

Broadly, a similar pattern is also observed when it comes to bank officials. Non-victims were more likely to report banks as 'very much trained' (27 per cent versus 22 per cent among victims), while victims were marginally more likely to view banks as 'not at all trained' (11 per cent versus 8 per cent among non- victims). However, among victims who separately complained to their bank, 26 per cent reported officials as very much trained, compared to 18 per cent among those who did not. This again shows a moderating effect of direct interaction with the institution.

The perception about the competence of judges or magistrates is also not very different. Non-victims (32 per cent) were more likely to view judges as 'very much trained' to deal with cybercrime compared to victims or those who assisted them (27 per cent). The latter group is also more inclined to perceive judges as not much trained (18 per cent versus 15 per cent) among non-victims. Among those whose cases reached court, 31 per cent of the victims said judges are very much trained, as opposed to 26 per cent of those whose cases did not go to court.

Likelihood of Reporting in the Future

Having examined perceptions about institutional police, bank officials and judges' competence, it is equally important to understand how these experiences and perceptions translate into future behaviour. Specifically, whether victims or the general public would choose to report a cybercrime if they encountered one.

To understand future reporting behaviour, a scenario was presented to the respondents. They were asked about their likelihood of reporting a case of cybercrime to the police if they become a victim in the future. Approximately half the respondents (48 per cent) reported a high likelihood. Thirty-five per cent said they are somewhat likely". Fourteen per cent say they are not likely to report in the future (11 per cent said "not much likely" and 3 per cent said "not at all likely").

When the respondents are asked about their likelihood of reporting cybercrime to the police in the future, there is a notable variation across different socio-economic groups. The most economically advantaged groups show the highest likelihood (58 per cent) of reporting future instances as opposed to those belonging to the poor category (40 per cent), with a difference of 18 percentage points between the two groups.

Steps Towards Digital Safety

Studying people's perceptions about who is responsible for data security and protection is important to hold institutions accountable. Responsibility for

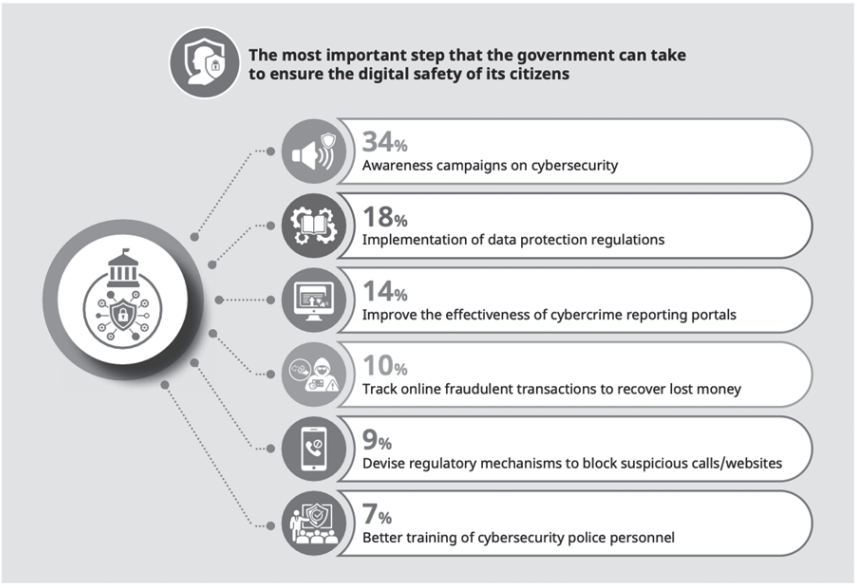
data protection is often shared between the individual and institutions, but how this balance is perceived by the public can influence people's behaviour.

While individuals protect their own information through everyday practices like using strong passwords, verifying app permissions and staying alert to risks, government or financial institutions, on the other hand, are expected to create secure systems that enforce systematic regulations and ensure that people are informed about how their data is used and protected.

To understand this balance and how it shapes perceptions about data regulation, respondents were presented with two statements and asked which one they agreed with the most. The data indicates that perceptions are relatively divided, with nearly half (45 per cent) saying it is the responsibility of the individual to protect their data, whereas another half (51 per cent) thought it to be the responsibility of the government or the bank authorities to ensure data protection and build public awareness.

While understanding where people place the burden of responsibility for digital safety offers valuable insight into public expectations, it raises a follow-up question: What do citizens expect the government to do? To this end, the respondents were asked what the most important step the government authorities can take to ensure the citizens' digital safety. The majority (34 per cent) said awareness campaigns on cybersecurity are the most important step that the government should undertake (Figure 14). This was followed by the need for the implementation of data protection regulations (18 per cent) and improving the effectiveness of cybercrime reporting portals (14 per cent). Only 7 per cent of the respondents felt that better training of cybersecurity personnel is the most important step that the government can undertake to ensure digital safety.

Figure 14: One-third of the respondents feel that the governments should launch an awareness campaign on cybersecurity



Note: The rest either cited other steps or did not respond. This was an open-ended question, and the answer categories were not read out.

Question asked: In your opinion, what is the most important step that the government/authorities can take to ensure the digital safety of the citizens?

Conclusion

Trust in digital financial infrastructure has emerged as a significant factor. As perceived safety with online banking channels declines, the burden of responsibility shifts decidedly from the individual towards the state. In terms of what citizens want for their digital safety, awareness campaigns are the most important step cited by a third of the respondents. This is followed by the implementation of data protection regulations and the improvement of the effectiveness of cybercrime portals.

Taken together, these findings suggest that confidence in the cybercrime security ecosystem is not at its best. To ensure that, the focus should not only be on strengthening the capacity of institutions that respond to cybercrime, but also on public confidence in those institutions.

IMPROVING SYSTEMIC RESPONSES

Recommendations from Victims and Experts

This article highlights key recommendations emerging from in-depth interviews with cybercrime victims and experts, as well as focus group discussions (FGDs). It presents edited excerpts from the recommendations detailed in Chapter 2 of *Status of Policing in India Report 2026: Cybercrime—Victim Experiences and Systemic Responses* .

Victims' accounts highlighted the need for greater institutional responsiveness, accessibility and accountability in the aftermath of cybercrime. Experts, including police personnel, banking professionals and civil society representatives, emphasised reforms to strengthen cybercrime prevention and investigation, improve access to justice, and enhance coordination and accountability across institutions.

Improving Reporting and Access to Justice

- **Simplifying the cybercrime reporting portal:** One victim of financial cyber fraud criticised the design of the National Cybercrime Reporting Portal (NCRP), observing that it should function more like other government digital services by guiding users through each stage of reporting, preventing incomplete submissions and allowing complaints to be saved and completed later.

- **Regular updates after the complaint:** Victims also highlighted the lack of transparency once complaints had been registered. One victim suggested that complainants should receive immediate confirmation that "your details are now with such and such agency", followed by regular updates on the case's status. Another recommended a tracking mechanism similar to the Right to Information process, enabling complainants to monitor each stage of the investigation rather than repeatedly contacting different agencies.

- **Editable complaints:** Victims also proposed that online complaints should remain editable so that additional information or evidence can be submitted without requiring repeated visits to police stations.

- **Dedicated reporting mechanisms for online gender-based crimes:** Experts working on gendered cybercrimes also highlighted the need to improve access to justice through dedicated reporting mechanisms, specialised support units and safeguards against coercive settlements for victims of gender-based cybercrimes.

> ***"The timeliness of institutional responses emerged as one of the most consistent concerns"***

Strengthening Institutional Response and Investigation

- **Defined timelines for registration and investigation:** The timeliness of institutional responses emerged as one of the most consistent concerns. Victims pointed to the need for clearly defined timelines for complaint registration and investigation, routine review of pending cases and stronger accountability mechanisms to ensure that cybercrime complaints receive timely attention.

- **Single-window mechanism:** The victims also pointed to the fragmented nature of the current institutional

response. Several victims said they had to separately visit police stations, banks, payment service providers, telecommunication companies and regulatory authorities after an incident of cyber fraud. To address this, victims recommended establishing a single-window mechanism capable of coordinating action across relevant institutions. Such a mechanism would reduce procedural delays, improve inter-agency coordination and minimise the burden currently placed on victims in navigating multiple institutions.

- **Improving technical and legal police infrastructure:** Across interviews, experts emphasised that the rapid growth and increasing sophistication of cybercrime have outpaced existing institutional capacity. Experts recommended expanding dedicated cybercrime police stations, strengthening cyber-forensic laboratories and investing in technological infrastructure to support digital investigations. Policing experts also highlighted the need to recruit investigators with engineering and cybersecurity expertise and recommended revisiting provisions of the Information Technology Act, 2000, that restrict the investigation of certain cyber offences to particular police ranks.

- **SOPs for inter-agency coordination in non-financial cybercrimes:** Civil society representatives recommended developing standard operating procedures that clearly define institutional responsibilities and improve coordination between police, regulators and victim support organisations.

- **Helpline for non-financial cybercrimes:** Experts also proposed establishing a dedicated 24-hour cybercrime helpline capable of providing immediate guidance, directing victims to the appropriate reporting mechanisms and ensuring that timely action is initiated during the critical period immediately following a cybercrime incident.

Accountability of Financial Institutions and Digital Platforms

- **More accountability of the banks:** One victim suggested that banks should monitor unusual transaction patterns, with additional verification for high-value amounts. Victims recommended that account holders should receive immediate notifications whenever accounts are flagged for suspected fraud. Victims also proposed allowing customers to determine transaction limits when opening bank accounts and introducing additional safeguards for vulnerable users. One victim recommended that transactions above a specified amount from a minor's account should require parental approval before completion. Another recommended that authentication systems should be reviewed and updated regularly to respond to emerging threats.

> ***"Banking experts, police personnel and civil society representatives argued that financial institutions, payment service providers and telecommunications companies should assume greater responsibility for preventing cyber-enabled fraud"***

- **Public disclosure of cyber-fraud statistics by the banks:** A victim recommended that banks periodically publish fraud statistics so that customers can compare institutions based on their cybercrime records.

- **Redistributing responsibility across institutions**: Experts also highlighted the need to redistribute responsibility for cybercrime prevention across institutions rather than placing the burden primarily on victims and law enforcement agencies. Banking experts, police personnel and civil society representatives argued that financial institutions, payment service providers and telecommunications companies should assume greater responsibility for pre-

venting cyber-enabled fraud. The expert argued that such measures encourage financial institutions to invest in stronger fraud prevention systems because institutional failures carry tangible consequences.

- **Strengthening regulatory bodies**: Experts recommended strengthening regulatory oversight of banks, payment intermediaries and telecommunications providers, particularly in relation to mule accounts, fraudulent SIM card issuance and other institutional vulnerabilities that facilitate cybercrime.

Strengthening Responses to Gender-based Cybercrimes

- **Gender-sensitive police response:** Victims of gender-based cybercrimes, including NCII abuse, bullying and sextortion, highlighted the need for responses that recognise the distinct nature of these harms. They emphasised that dismissive attitudes and victim-blaming responses by authorities can further compound trauma. They, therefore, recommended that police personnel should ensure that complaints are handled with empathy, confidentiality and respect for victims' dignity. They also advocated for specialised gender sensitive training for police officers and judicial personnel.

> ***"Experts recommended that police personnel should ensure that complaints are handled with empathy, confidentiality and respect for victims' dignity"***

- **Prompt action and improved inter-agency coordination:** Victims also stressed that quicker intervention is critical in cases where harmful content, abusive messages and intimate images can spread rapidly across digital platforms. They recommended stronger coordination between police, social media platforms and other intermediaries to facilitate the immediate removal of such content and prevent further circulation.

Expanding Cyber Safety Awareness and Prevention

- **Awareness campaigns:** Victims recommended practical awareness campaigns that explain common fraud techniques, safe digital banking practices, reporting procedures and the responsible use of digital payment applications, particularly for older adults, rural communities and first-time users. A banking expert stated that cyber safety campaigns should be delivered in regional and vernacular languages rather than relying primarily on Hindi and English.

- **Targeted training:** This included strengthening cyber safety education in schools, supporting parents and communities, and encouraging greater responsibility among technology companies.

COMMON CAUSE CASE UPDATES

Public Interest Litigations

Writ for Supreme Court Directions on Police Reforms (W.P. (C) 310/1996)

The battle for police reforms has been going on for the last 29 years. The Supreme Court (SC) took 10 years to give a historic judgment in 2006, in the petition filed by Prakash Singh, Common Cause and NK Singh IN 1996. Since then, it has been a struggle to get the Court's directions implemented. On July 3, 2018, responding to an interlocutory application filed by the Ministry of Home Affairs regarding the appointment of acting Director General of Police (DGP) in the States, the SC gave a slew of directions to ensure there were no distortions in such appointments. It laid down that the States shall send their proposals to UPSC three months before the retirement of the incumbent DGP. Despite clear directions, implementation across States on this issue remained inconsistent, resulting in recurring contempt and compliance proceedings before the Court.

On July 28, 2025, the court issued notice, and on August 18, 2025, the Court declined to entertain one of the contempt petitions, observing that the dispute appeared to arise from inter-personal rivalry between officers rather than a matter of public interest. This matter was listed several times from October 2025 till February 12, 2026. Two contempt petitions filed against the States of Telangana and Tamil Nadu were considered by the Court. The Court reiterated its previous order and directed that the States to comply with their previous directions.

On March 12, 2026, the Court disposed of civil contempt petition regarding the State of Tamil Nadu as infructuous and directed the UPSC to ensure the meeting regarding appointment of DGP be held on March 20, 2026, and recommendations be implemented without delay. Contempt petitions for the States of Bihar, Telangana and Andhra Pradesh were also disposed of for the reasons mainly associated with the UPSC recommendations.

It was brought to the notice of the Court that the State of Chhattisgarh had not appointed a regular DGP from the panel of recommended names by UPSC, and an acting DGP had been working since February 4, 2025. Since the UPSC had sought an explanation from the State Government on March 3, 2026, the Court, prior to taking any coercive action against the State authorities, issued notice to show cause as to why the UPSC recommendations of May 13, 2025, had not been implemented and why the acting DGP should not be restrained from performing the duty. Counsel for the State of Chhattisgarh sought and was granted six weeks' time to have instructions.

The States of Punjab, Manipur, Arunachal Pradesh, Goa and Mizoram were directed to show cause that, in the absence of any valid law having been enacted by them in terms of liberty granted by Prakash Singh (Supra), why appropriate action under the Contempt of Courts Act should not be taken for withholding recommendations for appointment of their respective DGPs out of the panel to be prepared by the UPSC. The counsel for Himachal Pradesh was granted six weeks' time to get instructions. The States of Jharkhand and Uttar Pradesh were directed to show cause as to why the proposal for the appointment of DGP as per Prakash Singh judgment had not been forwarded to UPSC. The counsels representing the State Governments/Union Territories were directed to submit a copy of their reply affidavit to Mr. Raju Ramchandran, learned Amicus Curiae, as well as to the counsel for the UPSC.

On May 19, 2026, the Court was apprised that a compliance affidavit had been filed by the States of Arunachal Pradesh and Chhattisgarh. As per the status

report filed by the UPSC, acting DGPs were working in Manipur and Jharkhand, and no proposal for appointment of regular DGPs had ever been received by the UPSC from them. As per the affidavit filed by the States of Punjab, Uttar Pradesh, Gujarat, and West Bengal, proposals had been received in March April and May 2026, respectively. The UPSC pointed out that no proposal had been received regarding Himachal Pradesh and the AGMUT cadre, pertaining to Arunachal Pradesh, Goa, and Mizoram. All the States, which, according to the UPSC, had not complied with the directions of this Court, were directed to file a compliance affidavit. The Court directed that the be listed for August 18, 2026.

On May 27, 2026, the application filed by the State of Manipur requesting appointment of DGP from outside Manipur cadre once the tenure of the acting DGP came to an end on May 31, allowed by the court. The said application had been filed narrating the unprecedented ethnic and civil unrest that had taken place in the State.

On May 29, 2026, the counsel for Karnataka brought to the notice of the Court that inadvertently, in the order of March 12, 2026, it could not be mentioned that the State had also complied with the direction of appointment of a regular DGP, on recommendations of the UPSC. The same was taken on record by the Court.

The appointment of Odisha's next DGP centered on the State Government's decision to widen the pool of officers who could be considered for the post by trying to include a relatively junior officer in the selection process in a manner that went against the SC's directions. Alleging that the DGP selection process was not in accordance with the Court's earlier directions, senior advocate Mr Chidambaram sought an urgent hearing before the SC. On August 13, 2026, the SC issued notice with directions for reply, if any, to be filed before the next date of hearing. The counsel for UPSC stated and assured the Court that in the intervening period no meeting of the empanelment committee would be convened.

This matter was listed several times during August and September 2026. During the hearing, the Supreme Court questioned the need for creating an ex-cadre post and adding more names when the UPSC had already recommended three eligible cadre officers under the Prakash Singh guidelines.

The State Government, represented by Solicitor General Tushar Mehta and Odisha Advocate General Pitambar Acharya, defended the decision, arguing that expanding the pool would provide a wider choice of suitable officers and that the process complied with the relevant Ministry of Home Affairs parameters and Supreme Court guidelines.

The hearing also examined the exclusion of senior IPS officer Sushant Kumar Nath from the selection process. His integrity certificate had been withdrawn by the State, a move that became one of the issues under scrutiny. The case also involved questions regarding the role of the UPSC, the eligibility of officers and the manner in which the panel should be prepared.

The bench, headed by the CJI took note of the detailed report submitted by Amicus Curiae Raju Ramachandran, which highlighted key operational discrepancies:

- The exclusion of senior IPS officer Sushant Kumar Nath from the initial eligibility pool;
- Questions regarding issuance of integrity certificates for candidate consideration; and,
- The procedural validity of adding officers promoted to the DG rank after the initial list had been submitted to the UPSC.

The arguments were concluded and on September 29, 2026, and the SC reserved its judgment in the matter. On October 8, 2026, the Centre challenged the appointment of Jharkhand DGP contending that the appointment violated the SC directions in the Prakash Singh case. The SC requested Amicus Curiae Raju Ramachandran to scrutinise nationwide breaches in the matter with the help of UPSC. The matter is likely to be listed on November 3, 2026.

M.A. in Writ petition on Illegal Mining in Odisha
(M.A. 18/2025)

In January 2025, Common Cause filed a Miscellaneous Application (MA) in the writ petition on Illegal Mining in Odisha. The MA prayed for directions to the State to expedite the recovery/attachment proceedings on an urgent basis by complying with directions contained in previous orders passed by the Supreme Court and to take immediate action to pursue all available remedies before the appropriate forum (Division bench of High Court or SLP before this Hon'ble Court) to have unfavourable orders reversed or altered. The MA was listed several times in January, February, March, April and May 2025.

The Interlocutory Application (IA) filed by Common Cause on February 23, 2023, focused on getting directives issued for the Union of India and the State of Odisha to impose limits on the extraction of minerals and on constituting a committee of two or three independent experts to suggest and recommend such limits and submit its report in a time-bound manner. The matter was disposed of by the Supreme Court on May 7, 2025.

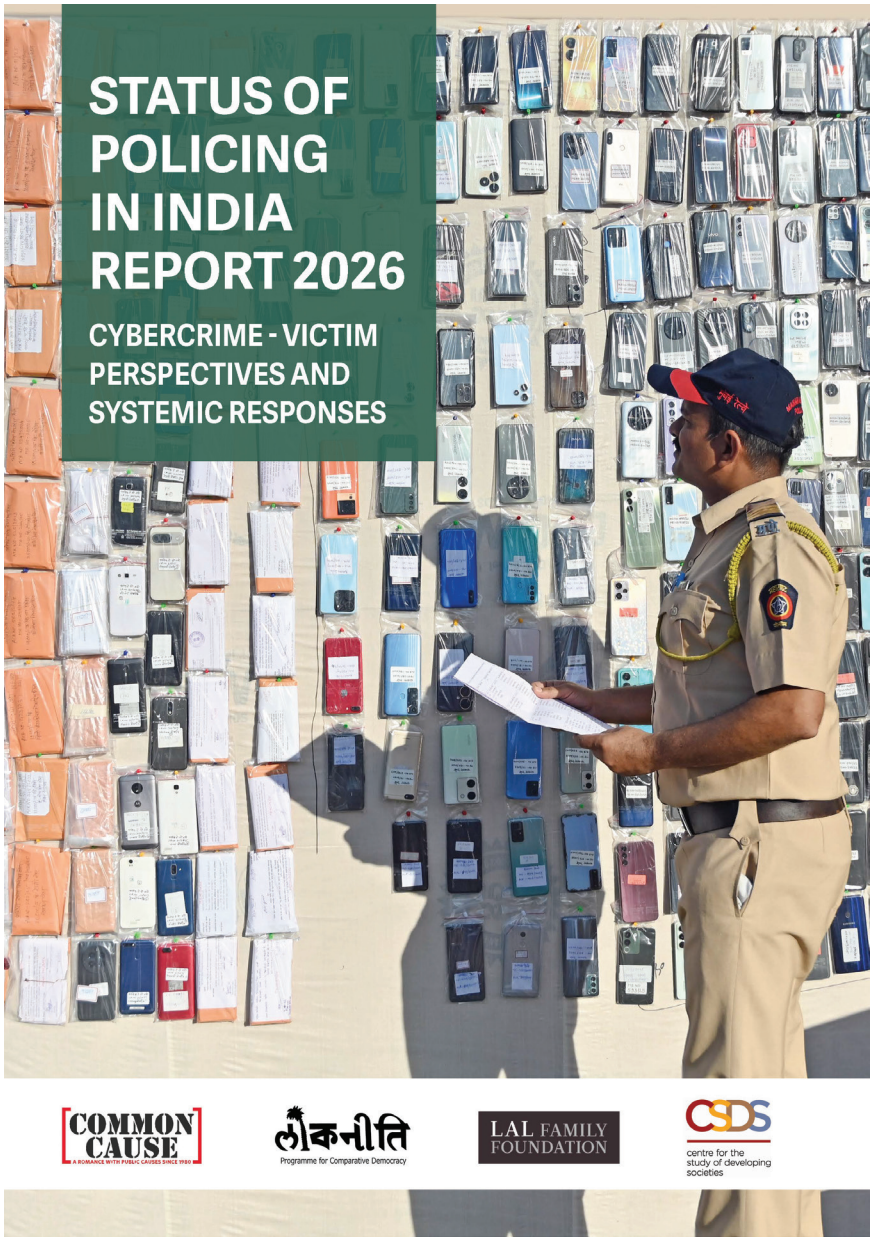
The IA also sought an updated status report on the amount of penalty deposited by the lessees, including the amount to be recovered, lease-wise details of the ore reserve, extraction permitted, the current status of the mining lease, total iron ore reserves and total permitted extraction in the State as directed in the judgment dated August 2, 2017. Significantly, the SC granted Common Cause, the petitioner, the liberty to file an independent writ petition for the same relief, which had been sought in the IA. It also granted the request that the State be called upon to file a status report on the points referred to in paragraphs 3 and 6 of the SC's order dated March 5, 2025, which is the prayer in the MA as well. The matter was directed to be listed in July 2025.

On July 28, 2025, a notice was issued, and Common Cause was granted liberty to serve the same through the Standing Counsel for the State. The MA was tagged with the Writ against the State of Odisha (W.P.(C) No. 675/2025) filed by Common Cause. Subsequent hearings on September 2 and September 17, 2025, addressed compliance issues, including extension of mining leases and joint inspection of mines. On December 10, 2025, the Court observed "We are informed that several writ petitions are pending before the High Court, wherein orders passed in recovery proceedings have been challenged and stay obtained." The Court directed that status report be filed on or before April 2, 2026 and MA and the connected matters be relisted in April second week.

This matter was taken up on March 24, 2026, when due to demise of the previous amicus curiae, Mr Rao, new amicus, Mr Gautam Narayan, was appointed by the court, and the parties were directed to provide all documents to Mr Narayan. The State of Orissa was directed to file affidavit in compliance with the order dated December 10, 2025. On April 21, 2026, and May 12, 2026 the matter was listed before the Court. On hearing the counsels, it directed the registry to re-list the matter in the week commencing July 20, 2026.

On July 20, 2026, the amicus curiae submitted two separate notes. The first note related to the status of all the MAs pending before the SC and the second note related to the aspect of recovery of monies in connection with the writ petitions pending before the Odisha HC at Cuttack. Time was given to the State till July 24, 2026, to present the facts in relation to the notes. On October 8, 2026, the Court issued a fresh directive regarding the ongoing miscellaneous applications filed by [Common Cause] and Prafulla Samantra. The Court officially instructed the CEC to step in and investigate the unresolved environmental degradation, non-compliance, and ongoing extraction violations in the critical mining belts of Keonjhar, Sundargarh, and Mayurbhanj districts. The matter is likely to be listed on December 8, 2026.

Please download from commoncause.in or email a request to commoncauseindia@gmail.com



The SPIR 2026 is a collaborative effort between Common Cause and Lokniti-CSDS. The report draws on a survey across 16 Indian states with over 8000 respondents, plus a series of focus group discussions and in-depth interviews. It examines India's evolving cybercrime landscape and the institutional mechanisms meant to address it.

This study investigates experiences and patterns of victimisation in offences such as online fraud, digital arrests, trolling and bullying, identity theft, and online sexual harassment. It also examines how victims engage with reporting mechanisms, the role of banks and other institutions, and the challenges the victims encounter in securing remedies and justice.

Printed & Published by Vipul Mudgal on behalf of Common Cause, 5 Institutional Area, Nelson Mandela Road, Vasant Kunj, New Delhi 110070, Printed at PRINTWORKS, C-94, Okhla Industrial Area, Phase - 1, New Delhi - 110020
Editor-Vipul Mudgal Tel No. 26131313, 45152796, email: commoncauseindia@gmail.com, website:www.commoncause.in