# NHRC, India organises an Open House Discussion on 'Safeguarding human rights against digital arrest scams' in hybrid mode

## Chairing the discussion, NHRC Chairperson, Justice V. Ramasubramanian highlights cyber-enabled frauds threatening rights, dignity and security of individuals

## Member, Justice (Dr.) Bidyut Ranjan Sarangi underscores gaps in existing processes to address the challenges posed by digital frauds

## Member, Smt. Vijaya Bharathi Sayani says, preventive action is not only a matter of technology and regulation but also a responsibility of good governance

## Secretary General, Shri Bharat Lal says, cybercriminals are increasingly exploiting personal data obtained through data leaks and other sources to target vulnerable people, raising serious concerns about data privacy and protection

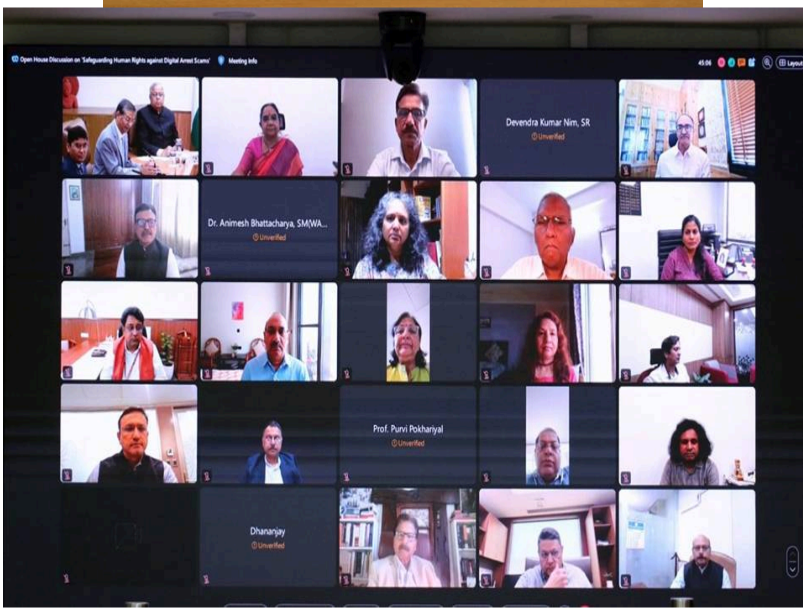
## Among various suggestions, recognising digital arrest scams as a distinct offence under the existing legal framework to facilitate more effective investigation, prosecution and victim redressal highlighted

प्रविष्टि तिथि: 09 JUN 2026 7:48PM by PIB Delhi

The National Human Rights Commission (NHRC), India today organised an Open House Discussion on 'Safeguarding human rights against digital arrest scams' in hybrid mode at Manav Adhikar Bhavan, New Delhi. Chairing the discussion, Justice V. Ramasubramanian, Chairperson highlighted the growing threat posed by cyber-enabled frauds, particularly digital arrest scams and underscored their serious impact on the rights, dignity and security of individuals. NHRC Members, Justice (Dr.) Bidyut Ranjan Sarangi, Smt. Vijaya Bharathi Sayani; Secretary General, Shri Bharat Lal; Director General (Investigation), Smt. Anupama Nilekar Chandra; Joint Secretary, Shri Samir Kumar; Core Group members, Special Rapporteurs, Special Monitors, senior functionaries representing different key departments of Government of India including Ministry of Electronics & Information Technology (MeitY), Ministry of

Telecommunications, Telecom Regulatory Authority of India (TRAI), Reserve Bank of India (RBI), CBI, National Payment Corporation of India, eminent legal and domain experts, representatives of Telecom operators and Banking and Fintech Associations participated in the discussion.

Chairperson, NHRC Justice V. Ramasubramanian emphasised the need for a collective response to tackle the menace. He noted that Indians have lost about Rs 52,976 crore to cyber-enabled frauds during the past six years, with nearly 8 per cent of the losses attributed to digital arrest scams. The data has been reportedly compiled by the Indian Cyber Crime Coordination Centre (I4C) based on the National Cyber Crime Reporting Portal. He observed that in many reported cases, the scamsters coerced their victims into transferring money by exploiting the fear of law enforcement agencies among people.


He also pointed out that the victims face significant challenges in recovering even a part of the amount, as the legal and procedural processes proved lengthy, costly and distressing. At times, the process of recovery becomes more painful than the process of losing money. The Chairperson further said that there are reports of lakhs of mule accounts in the country, which facilitate the movement of fraudulently obtained funds. Stressing the need to protect victims and uphold their rights, he called for practical suggestions on preventing such frauds. He said it will be necessary to improve recovery mechanisms, restore victims' financial security and help them regain their status in life and peace of mind by identifying and plugging loopholes in the legal framework, improving the response of law enforcement agencies and developing standard operating procedures to tackle digital arrest scams. He also suggested exploring mechanisms such as alerts on prolonged OTT calls to protect citizens from digital fraud.

NHRC Member, Justice (Dr.) Bidyut Ranjan Sarangi said that there are gaps in existing processes to address the challenges posed by digital fraud. He expressed the hope that such discussions are expected to help in developing practical solutions at the earliest. Member, Smt. Vijaya Bharathi Sayani emphasised that safeguarding citizens from cybercrime and financial fraud is an essential extension of Rajadharma. Preventive action is not only a matter of technology and regulation but also a responsibility of good governance. Therefore, our collective goal should be to ensure that no one becomes a victim of such frauds.


Earlier, NHRC Secretary General, Shri Bharat Lal, in his opening remarks, spoke about the background of convening the Open House Discussion on ‘Safeguarding human rights against digital arrest scams.’ He said that cybercrimes mostly affect elderly persons, including retired government officials, professionals, industrialists and bankers, causing not only financial losses but also compromising their dignity, self-respect and psychological well-being. Referring to information placed before the Supreme Court in a related matter, he said that more than 3,000 such frauds targeting elderly persons were reported last year.


He said that cybercriminals are increasingly exploiting personal data obtained through data leaks and other sources to target victims, raising serious concerns about data privacy and protection. Evolving digital governance and financial systems enable them to commit fraud and move money faster uncaught. He urged strengthening safeguards to protect vulnerable groups, particularly senior citizens and ensuring effective support and remedies for victims of cyber fraud.

Shri Lal said that the Commission has divided the subject into three technical sessions for discussion to find a way forward. These are: a.) identify the drivers behind the surge in digital arrest scams and the constraints limiting effective response, b.) formulating preventive measures to address digital arrest scams, and c.) enhancement of grievance redressal, compensation and victim assistance mechanisms. He requested the experts to share their insights on these aspects for Commission to firm up its response.

Giving an overview of the government's efforts in the matter of checking digital scams, Shri Ajit Kumar, Joint Secretary, MeitY said that an inter-departmental committee is examining measures to address digital arrest scams from prevention to compensation. He also informed that a portal is being developed under Section 47 of the IT Act to facilitate adjudication and compensation and expressed confidence that implementation of the DPDP framework would strengthen protection of citizens' data and help address data-related concerns.

Ms. Roopa M., Inspector General of Police, Indian Cyber Crime Coordination Centre (I4C) highlighted the cybercrime.gov.in portal, helpline 1930 and the CFCFRMS platform for tracing, holding and restoring funds to victims. She also called for stronger action against the misuse of government logos, SIM boxes and mule accounts. Shri Muktesh Chander, Special Monitor, NHRC stressed the need to regulate SIM cards and bank accounts, address the psychological fear exploited by fraudsters, ensure FIR registration in cyber fraud cases and adopt a victim-centric approach instead of victim blaming. Shri Brijesh Singh, ADG, Maharashtra described cybercrime as an industrial-scale operation enabled by data breaches, mule networks and AI. He advocated automated golden-hour intervention, a national cybercrime force, stronger DPDP enforcement, victim compensation and psychological support.


Shri R. Vanaraja, Chief General Manager, Department of Information Technology, RBI highlighted the potential of artificial intelligence to identify patterns in digital arrest crimes and generate alerts and suggested exploring a single government communication channel. He also emphasised the need to raise public awareness against misuse of bank accounts and the need to balance fraud prevention with convenience for genuine users. Shri Rajiv Ranjan Prasad, Senior Advisor, IBA highlighted measures taken by the banking industry to prevent digital frauds, including AI-based detection of mule accounts, the Beneficiary Account Name Lookup Facility and the proposed Indian Digital Payment Intelligence Platform. He also referred to the RBI's proposal for a 'trusted person' mechanism to provide additional authentication for high-value transactions by vulnerable customers.

Shri Ramesh Krishnamurthy, Chief Risk Management, NPCI highlighted NPCI's efforts in customer education, including awareness campaigns and outreach in villages, as well as AI-based fraud monitoring and real-time support to law enforcement agencies. He emphasised the need for a concerted response by all stakeholders to tackle digital fraud.

Shri Sanjeev Kumar Sharma, Deputy Director General (AI & Digital Intelligence Unit), Department of Telecommunications outlined preventive measures such as the Sanchar Saathi initiative, AI-based tools, international call spoofing detection and the Digital Intelligence Platform. He emphasised stronger regulation of OTT platforms, real-time data sharing and improved complaint-to-FIR conversion to deter cyber frauds. Ms. Astha Modi, SP, CBI said that large-scale digital arrest scams originate from cyber scam compounds in Southeast Asia and are sustained by mule accounts, telecom infrastructure, social media intermediaries and human trafficking. She outlined CBI's action against mule account networks, telecom infrastructure, social media intermediaries and human trafficking networks and referred to an AI-based chatbot for verification of CBI notices and summons.

Shri Ashok Kumar, Joint Advisor, TRAI flagged the urgent need to bring OTT communication platforms used for voice calls, messages and video calls under an appropriate regulatory mechanism, noting that most digital arrest frauds have shifted to OTT channels. He also suggested measures such as alerts or interruptions during unusually long calls to help prevent digital arrest scams. Major Vineet Kumar, Founder and Global President of Cyber Peace Foundation advocated a model of shared responsibility involving government, industry, academia, civil society and citizens and called for the creation of a 'human firewall' of trained first responders. He also emphasised psychological support for cybercrime survivors and rehabilitation measures for first-time cyber offenders and juveniles.


Ms. N. S. Nappinai, Senior Advocate, Supreme Court highlighted the human rights dimensions of digital arrest scams, including human trafficking, violations of privacy, life and liberty and psychological trauma. She emphasised restorative justice, victims' rights of recompense and shared liability frameworks. Dr. Pavan Duggal, Advocate, Supreme Court said that digital arrest is not a specific offence under existing laws and suggested its incorporation as a distinct crime under the Information Technology Act, 2000 or the Bharatiya Nyaya Sanhita. He also called for a statutory 'circuit breaker' for high-value transactions, a Digital Arrest Victims Fund, recognition of digital arrest as a human rights issue and stronger measures to address violations of dignity, privacy and mental integrity caused by such scams.

Shri Rahul Vatts, Chief Regulatory Officer, Airtel said that 97–98 per cent of customer onboarding is carried out through Aadhaar KYC, supported by live photographs and biometric authentication at points of sale (POS). He highlighted the use of AI to identify suspected spam calls and SMS in 14 different languages, detect and block fraudulent links, and issue alerts when an OTP is shared during an ongoing call.

Smt. Anupama Nilekar Chandra, DG (I), NHRC said that cybercrime has emerged as a new dimension alongside drug trafficking and human trafficking, with over one billion mobile users potentially vulnerable to digital frauds. She suggested that NHRC could constitute theme-based sub-committees to examine legal loopholes, inter-agency coordination, capacity building, rehabilitation and compensation for victims.

Some of the other suggestions that emanated from the discussions are as follows:

- Digital arrest scams may be recognised as a distinct offence under the existing legal framework to facilitate more effective investigation, prosecution and victim redressal;
- The legal framework may be strengthened by explicitly criminalising the renting of mule accounts, trafficking for forced criminality and misuse of government logos for fraudulent purposes;
- Automated safeguards such as transaction ‘circuit breakers’, trusted-person authentication, temporary suspension of suspicious transactions and alerts during prolonged calls may be explored to prevent coercive transfers of funds;
- Recovery and restoration mechanisms for victims need to be simplified and expedited to reduce procedural delays and hardships;
- Greater accountability may be introduced across the digital ecosystem, including financial institutions, telecom operators, intermediaries and service providers to strengthen fraud prevention and response;
- The adjudication mechanism under the Information Technology Act may be strengthened to facilitate victim redressal and accountability of intermediaries;
- Dedicated compensation and support mechanisms may be considered for victims who suffer substantial financial and psychological harm;
- Systems for proactive identification and alerting of potential victims may be developed through analysis of transaction patterns and coordinated information-sharing among stakeholders;
- A single government communication channel or verification portal may be explored to enable citizens to verify the authenticity of law enforcement credentials, notices and communications;
- Need for special measures to address the misuse of emerging technologies, including artificial intelligence, deepfakes and synthetic identities, for cyber-enabled frauds;
- Stronger safeguards should be developed to protect senior citizens and other vulnerable groups who are mostly targeted by digital arrest scams;
- International cooperation should be strengthened to disrupt transnational cybercrime networks and cyber scam compounds operating across jurisdictions;
- Public awareness initiatives should focus on behavioural manipulation tactics used by fraudsters, including impersonation, intimidation and exploitation of trust in authority;
- Enhanced training and capacity building for law enforcement agencies, financial institutions and frontline responders should be undertaken to improve prevention, investigation and victim assistance;
- Developing a mechanism to ensure that law enforcement agencies have timely access to the contact details of grievance officers and compliance officers of intermediaries for data requests, summons and takedown actions.

The Commission will further deliberate on these suggestions to finalise its recommendations to the Union and State Governments.

*****

**NSK**

(रिलीज़ आईडी: 2270875) आगंतुक पटल : 370
इस विज्ञप्ति को इन भाषाओं में पढ़ें: Urdu , Tamil