National Human Rights Commission, India

Minutes of the Open House Discussion

On

Safeguarding Human Rights Against Digital Arrest Scams

09 June 2026

1. The National Human Rights Commission organised an Open House Discussion on '*Safeguarding Human Rights against Digital Arrest Scams'* on 09 June 2026, in hybrid mode. The discussion was chaired by Justice Shri V. Ramasubramanian, Hon'ble Chairperson, NHRC and attended by Hon'ble Members Justice (Dr.) Bidyut Ranjan Sarangi and Smt Vijaya Bharathi Sayani. Shri Bharat Lal, Secretary General; Smt. Anupama Nilekar Chandra, Director General (Investigation); Shri Samir Kumar, Joint Secretary, NHRC, were also present in the meeting. Representatives from various government institutions, Associations, non-governmental organisations (NGOs), private bodies and domain experts, along with Special Monitors and Special Rapporteur, also attended the meeting. The list of participants is annexed.

2. The discussion was structured around three agenda items, i.) Identify the drivers behind the surge in digital arrest scams and the constraints limiting effective response; ii.) Formulating Preventive Measures to address Digital Arrest Scams; and iii.) Enhancement of grievance redressal, compensation, and victim assistance mechanisms.

3. At the outset, **Shri Samir Kumar, Joint Secretary, NHRC**, welcomed all participants. Citing the example of an imminent business leader who was defrauded of ₹7 crore, he illustrated the severity of the issue in which everyone is vulnerable. Noting the presence of representatives from diverse backgrounds, he emphasised that addressing this challenge would require collective action and coordinated efforts.

4. In his opening remarks, **Shri Bharat Lal, Secretary General, NHRC**, underscored the importance of focused deliberation on digital arrest scams, noting the increasing incidence and wide impact. He pointed out that even highly educated individuals and seasoned professionals are falling victim to such frauds, dispelling any notion that vulnerability is limited to the uninformed. Referring to data placed before the Supreme Court, he highlighted that losses exceeding ₹3,000 crore have already been recorded, with elderly citizens being the primary target. He pointed to data leakage as a key contributor, supplying scammers with personal information which they then leverage against the victims. He also emphasised upon the human rights implications of digital arrest, before outlining the day's agenda and inviting stakeholders to share their actionable suggestions.

5. In his inaugural address, **Justice Shri V. Ramasubramanian, Hon'ble Chairperson, NHRC**, observed that people largely follow the law out of fear of enforcement rather than principle, a psyche that fraudsters exploit when a person in uniform appears on screen. Citing statistics, he noted that Indians have lost approximately ₹52,976 crore to cyber frauds over six years. He illustrated the challenges in fund recovery through the example of an acquaintance who lost ₹1.17 crore in a span of three years in such a fraud, with the money routed through 735 accounts, including several foreign accounts. Of this amount, authorities were able to freeze only a few lakh rupees, and the victim was subjected to a complicated and protracted process in attempting to recover the funds. He further observed that victims often struggle even to establish their own identity against the fraudsters' fabricated ones. Noting that around 8.5 lakh mule accounts are estimated to be operating in the country, he invited participants to reflect on NHRC's role in preventing such frauds and helping victims regain their money, dignity, and peace of mind.

6. **Smt Roopa M, IG, I4C**, informed participants that I4C forwards complaints received through the National Cyber Crime Reporting Portal and the 1930 helpline to the jurisdictional police stations concerned for action. She stressed that timely fund tracing is the most critical aspect in digital arrest cases, highlighting the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) as the backend mechanism enabling this. On fund restoration, she noted the absence of a uniform mechanism for returning recovered funds to victims, which led I4C, in coordination with MHA, to develop a Standard Operating Procedure (SOP). This SOP has since been placed before the Hon'ble Supreme Court, resulting in the piloting of a Money Restoration Module and a Grievance Redressal Module. She flagged three areas requiring tighter regulation: communication platforms, misused for scam calls and impersonation through unauthorised use of law enforcement logos; telecom infrastructure, particularly the misuse of SIM boxes; and banks, where flagged or suspicious transactions often do not see swift suspension action. She also informed that I4C is working with RBI on a compensation framework for authorised push-payment frauds. She also pointed to a few legislative and institutional gaps: the absence of a statutory provision criminalising the renting or sale of mule accounts, statutory provision to enable real-time suspension of suspicious accounts; explicit legal recognition of trafficking to foreign scam compounds; the need to strengthen adjudication under Section 46 of the IT Act; and the need for better intermediary accountability, given that many intermediaries lack accessible nodal officers in India. She concluded by recommending a unified portal of verified law enforcement credentials, and wider sharing of red-flag indicators among stakeholders for coordinated detection.

7. **Muktesh Chander, Special Monitor, NHRC**, noted that fraudsters rely on two key tools, viz., SIM cards and bank accounts, yet, unlike firearms, these remain poorly regulated. He highlighted the psychological fear tactics used in these scams as a factor. He pointed out widespread public unawareness of basic legal concepts that seizure requires physical seizure, and that "digital arrest" has no legal basis, compounded by weak deterrence due to poor traceability of accused persons via SIM cards or bank accounts. He flagged the low conversion rate of complaints to FIRs (estimated at 5–

10%), citing lack of a clear conversion mechanism as a potential source of corruption, and called for automatic FIR registration once certain criteria are met. He proposed that serious cyber crimes above a certain threshold be automatically routed to a central agency like the CBI, given that individual investigating officers are overburdened and unable to handle nationwide travel and caseloads. He also called for addressing the victim-blaming tendency and stressed upon that victims deserve sympathy, not blame, and suggested the NHRC to take up such serious cybercrime complaints and hold states accountable for FIR registration and recovery action. He concluded by pointing to AI's potential in tracking financial flows and identifying suspects.

8. **Shri Brajesh Singh, ADG, Maharashtra,** stated that cybercrime operates on an industrial scale, where target profiles from data breaches are sold to fraudsters prior to initial contact. He explained that syndicates utilise cognitive hijacking or Android malware to siphon funds through multi-level mule networks and hybrid crypto-hawala channels within 30 minutes, whereas state investigations face bottlenecks like Mutual Legal Assistance Treaties (MLATs), taking an average of 1,300 days. Highlighting the low entry barriers and generative AI plugins that allow live voice impersonation, he noted a double-victimisation crisis where roughly 30,000 Indian IT professionals have been trafficked under false pretences into vast, city-sized scam compounds in Cambodia, Laos, and Myanmar. To counter this, he urged for an automated, API-driven golden hour protocol, mule account suppression via tracking anomalous outgoing-only SIM box data, and the strict enforcement of the Digital Personal Data Protection (DPDP) Act against high-risk fiduciaries like fintechs and data brokers. He concluded by recommending the establishment of a centralised National Cybercrime Force with end-to-end operational visibility, a single authenticated government communication layer to eliminate institutional impersonation, and

expanded victim frameworks integrating psychological support and structural financial compensation to protect the integrity of India's Digital Public Infrastructure.

9. **Shri Ajit Kumar, Joint Secretary, Ministry of Electronics and Information Technology**, informed that digital arrest scams form a significant share of reported cyber frauds, with apprehending perpetrators remaining difficult given their transnational, tech-driven nature, underscoring the need to explore victim compensation mechanisms. He informed that, on Supreme Court directions, a sub-committee chaired by the Special Secretary, MHA, with representatives from MeitY, I4C, and MHA among others, is deliberating comprehensive measures. He flagged persistent technical challenges, including SIM box misuse and telecom infrastructure gaps. He noted that Section 46 of the IT Act empowers adjudicating officers to award compensation, and that a dedicated portal, under development with C-DAC Noida, is being built to let victims approach adjudicating authorities directly, reducing procedural delays, with claims up to ₹5 crore adjudicable under the existing IT Act framework. He also noted that the DPDP Act's phased implementation would strengthen data protection safeguards and reduce vulnerabilities exploited by cybercriminals. He concluded by expressing optimism that the Supreme Court-mandated committee would deliver practical solutions and acknowledged NHRC's engagement as a valuable contribution to safeguarding victims' rights.

10. **Ms. N. S. Nappinai, Senior Advocate, Supreme Court of India,** raised the issue of cyber scam compounds, where individuals are trafficked across borders on false job promises and forced into cyber fraud. She urged the NHRC to investigate human trafficking of Indian jobseekers sent to overseas compounds, where their native accents are exploited as tools against local targets. Highlighting severe violations of privacy and liberty under Article 21, she cited a case where a victim was held under digital arrest for over a month and forced to keep 24/7 active audio mode even in restrooms, causing lifelong trauma. To combat siphoning where only 5% of funds are recovered, she advocated for a comprehensive restorative justice system based on global Authorized Push Payment (APP) models; this includes a shared-liability framework to recover 90% to 95% of losses by holding social media intermediaries, telecom service providers, unverified PoS agents, and banks financially accountable. She strongly recommended an automated communication "kill-switch" to systematically terminate prolonged, unnatural audio-video streams on apps like WhatsApp or Skype, effectively breaking the psychological hold of fraudsters to allow family or actual police to intervene.

11. **Shri R Vanaraja, Chief General Manager, Department of Information Technology, Reserve Bank of India** endorsed the idea of advancing the unified government communication layer by expanding the DoT's recent 1600-series banking protocols to encompass a standardized number for all state agencies, alongside integrating a single public-facing government domain extension similar to the new 'bank.in' banking framework. Regarding delayed credits via RTGS or NEFT, he clarified that since these systems clear at the central bank level as interbank settlements, any statutory delay mechanism must be mathematically executed at the initial customer-transaction phase before hitting the central settlement rail. He proposed that telecom and internet intermediaries utilise historical digital arrest datasets to train predictive AI models capable of recognising anomalous, continuous call patterns such as long-duration WhatsApp audio-video streams, to automatically trigger network alerts. Finally, while supporting the active MHA-RBI "Mule Hunter" project, he urged for grassroots awareness campaigns targeting unaware mule account holders paired with strict transaction balancing rules to prevent false-positive account freezes from inconveniencing and irritating genuine users transacting within their standard legal limits.

12. **Shri Sanjeev Kumar Sharma, Deputy Director General, DoT**, highlighted that the sheer operational cost of investigating isolated, low-value digital scams makes proactive prevention a critical imperative for all state agencies. To counter traditional calling line spoofing where Southeast Asian syndicates mask international calls as domestic numbers to impersonate premier entities, he detailed the implementation of a real-time scrubbing technology at international gateways that cross-references calls with active outbound

data. This technical solution systematically intercepts and drops unverified spoofed connections, dropping 1.35 million illegal incoming streams in its initial 24 hours and driving an immediate 99% reduction in traditional network telecom spoofing. Under the *Jan Bhagidari* model, he explained that the DoT crowdsources data through the *Sanchar Saathi* portal and application, utilizing 1 million reported citizen data points to automatically disconnect over 4.5 million suspicious connections. Furthermore, he detailed that the AI-driven *ASTR* tool enforces facial de-duplication across trillions of dynamic customer identification records to identify mass fraud patterns, a capability that has already led to the disconnection of 8.5 million fraudulent connections. To overcome the siloed execution of post-incident responses, he outlined the Digital Intelligence Platform, a unified system linking 1,500 entities including the CBI, state police forces, and over 1,300 banking institutions to securely share cross-network suspect data and run multivariate AI threat evaluations. He concluded by warning that because these extensive network-level interventions have restricted traditional telecom channels, syndicates have rapidly migrated 80% to 85% of their fraudulent operations to unregulated OTT media, necessitating the urgent introduction of telecom-grade statutory regulations to oversee digital communication intermediaries.

13. **Ms. Astha Modi, SP, Cyber Division, CBI** stated that large-scale digital arrest scams systematically originate from highly structured, corporate-style compounds in Southeast Asia that exploit local political instability and regional militias to run industrial-scale operations. To manage resources effectively, she noted that the inter-departmental committee and the Supreme Court of India established a jurisdictional threshold directing the CBI to investigate cases exceeding ₹10 crores. She outlined that the cybercrime ecosystem rests on four critical pillars:
    - Financial pillar utilizing domestic mule accounts, cryptocurrency channels, and complicit bankers to siphon funds;
    - Telecom pillar exploiting compromised Points of Sale (PoS) and SIM boxes to mask call origins;
    - Social media intermediaries—including WhatsApp, Skype, Telegram, Signal, and Microsoft Teams—used to locate victims and impersonate apex institutions like the CBI and the Supreme Court; and a
    - Human Trafficking pillar where individuals are lured, subjected to lethal 24/ 7 surveillance, and abused to exploit their cultural and linguistic familiarity for social engineering.

    To safeguard institutional public trust, she highlighted that the CBI has deployed an AI-based website chatbot integrated with its automated backend database, allowing citizens to instantly cross-reference and verify the authenticity of uploaded summonses, a simple, scalable solution she urged should be replicated across all Indian law enforcement agencies and judicial setups.

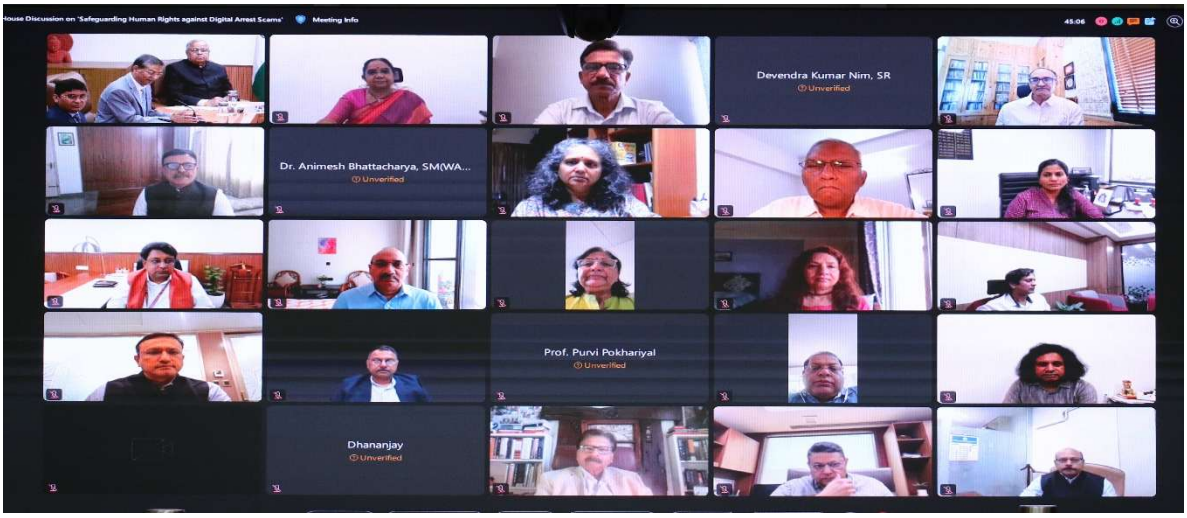
14. **Shri Ashok Kumar, Joint Advisor, TRAI** pointed out that while extensive rules exist for traditional telecom channels including the recent introduction of the 1600 series to secure financial

transactions, Over-The-Top (OTT) communication platforms, on which scammers have largely shifted operate as parallel networks for voice, video, and messaging remains unregulated. To address this regulatory gap, he emphasised the urgent need to bring communication-focused OTT platforms under a regulatory mechanism, noting that existing IT rules remain limited to content moderation rather than communication oversight. Drawing on his experience at the I4C, he stated that despite MHA flagging this shift to the MeitY as early as 2022, regulatory enforcement remains constrained, as evidenced by platforms like Truecaller defying TRAI directives by continuing to crowdsource spam tags on legitimate 1600-series banking calls under the pretext of jurisdictional exemption. To disrupt the prolonged psychological manipulation characteristic of digital arrests, he shared that TRAI recently engaged with WhatsApp to propose collaborative, technical interventions, such as injecting automated beep sounds or alarms during long, uninterrupted calls to break the victim's isolation. He concluded by emphasising precise regulatory measures to onboard and govern OTT intermediaries effectively.

15. **Major Vineet Kumar, President, CyberPeace Foundation**, emphasised that combating digital arrest scams requires a framework of shared responsibility across industry, academia, civil society, government, and netizens. To move beyond traditional checklists, he advocated for building a "human firewall" by training NCC, NSS, and NYKS cohorts as local first responders to provide informal reporting mechanisms and counter the social stigma associated with police reporting. Addressing critical gaps in grievance redressal, he pointed out that survivors in regions like Bihar and West Bengal face severe linguistic barriers on current portals, urging for the deployment of a multilingual chatbot for platforms like 1930 and cybercrime.gov.in to accommodate people with limited literacy. Regarding criminal disruption, he drew from his field experience in Jamtara to explain that young, first-time offenders and juveniles are often driven by lifestyle aspirations and face worse criminalisation inside standard detention facilities; consequently, he recommended establishing a specialised Cyber Rehabilitation Centres modelled. Finally, to mitigate the severe psychological trauma and suicide risks among victims, he detailed CyberPeace's "Cyber Heal" initiative with NIMHANS and called for an expanded, institutionalised victim protection framework that integrates psychological counselling, simplified legal redressal, and financial compensation.

16. **Shri Ramesh Krishnamoorthy, Chief Risk Officer, NPCI,** highlighted that digital arrest scams exploit psychological triggers by creating urgency and authority to coerce victims into high-pressure financial transactions. Operating as a network provider without direct customer

profiles, he explained that NPCI relies on a collaborative approach with banks, Telecom Service Providers, and the Indian Cyber Crime Coordination Centre (I4C). To counter these threats, he outlined NPCI's multi-layered framework, which includes pan-India awareness campaigns via mass television ads, print media, and rural *Nukkad Nataks*. Finally, regarding proposed measures like delayed financial credits, he cautioned that they offer limited effectiveness in cases of absolute coercion, risk disrupting genuine customer transactions, and could unintentionally push transactions toward less traceable channels, reaffirming that the focus must remain on risk-based preventive monitoring and 24/7 API data sharing with law enforcement.



17. **Dr. Pavan Duggal, Advocate, Supreme Court of India**, noted that digital arrest is not recognised as a specific offence under Indian law, leaving complaints often unregistered or filed under unrelated sections. He recommended making it a distinct offence under the IT Act, 2000, or the Bharatiya Nyaya Sanhita, 2023. He argued banks cannot claim ignorance of such transfers, and called for clearly defining banks' intermediary obligations under Section 2(1)(w) of the IT Act, given their existing due diligence duty under Section 79(2)(c). He proposed a statutory circuit-breaker requiring banks to delay transfers above ₹5–10 lakh by 2–3 hours to allow timely reporting, and a Digital Arrest Victims Fund financed by stakeholders in the transfer chain, with non-compliant banks losing Section 79 exemption. He urged the Commission to pivot the narrative from blaming a "gullible mind" to recognising digital arrest as a gross violation of fundamental human rights under Article 21, pointing out that the lifelong stigma, shame, and invasion of mental and digital dignity require specialised online rehabilitation and psychological counselling. Finally, he warned against the regulatory vacuum surrounding deepfakes and generative AI used by syndicates to create convincing law enforcement avatars, disproportionately trapping isolated senior citizens and women due to a culturally ingrained fear of authority uniforms. He recommended stronger procedures, quicker convictions under existing

provisions like extortion and Section 66D of the IT Act, and a high-level panel on the human rights dimensions, stressing focus on citizen dignity over conviction rates.

18. **Shri Rahul Vatts, Chief Regulatory Officer, Bharti Airtel** observed that digital fraud has evolved into an industrialised, transnational, AI-assisted business model. He informed that 97-98% of telecom onboarding now uses Aadhaar-based KYC with live image verification, backed by biometric authentication at points of sale. Airtel has deployed a new technology that has successfully detected 86.7 billion spam calls, flagged 3.6 billion spam messages, and blocked 1.26 million fraudulent links, alongside a recently launched OTP fraud detection system that warns users in real-time if an OTP is requested during an active call. He pointed out that a significant volume of spam now originates on unregulated messaging OTT platforms that lack direct subscriber accountability, creating severe regulatory asymmetry. To resolve this fragmentation, he urged authorities to establish a Unified National Communication Safety Framework that enforces proportionate, risk-based safeguards across all mass outreach digital platforms irrespective of the underlying technology.

19. **Shri Rajeev Prasad, Senior Advisor, IBA,** highlighted that the banking industry, partnering with the RBI, NPCI, and law enforcement, has deployed predictive AI models to detect mule accounts, monitor sudden turnover spikes, and execute Enhanced Due Diligence.To block fraudulent outreach, he noted that banks work with TRAI to enforce strict whitelisting protocols, ensuring unverified URLs and SMS headers cannot reach customers. Addressing specific counters to digital arrest scams, he referenced an RBI discussion paper proposing a "trusted person" authentication layer to validate transactions over ₹50,000 for vulnerable senior citizens aged 70 and above. He concluded by stating that while technical controls like transaction kill-switches, lagged credits, and low-credit categorisation thresholds of ₹25 lakhs are being evaluated, branch-level bank staff remain highly effective, having proactively intercepted multiple live digital arrest scams by identifying high-stress behavioural anomalies in victims.

20. **Ms. Anupama Nilekar Chandra, DG, NHRC** classified cybercrime as a critical third dimension of transnational organised crime alongside drug and human trafficking, elevated by an unprecedented scale targeting over one billion Indian mobile users. To systematically address this growing crisis, she recommended that the NHRC may actively take up the issue by constituting specialised, theme-based subcommittees. These subcommittees would be mandated to focus on plugging critical legal loopholes, streamlining real-time inter-agency coordination, enhancing law enforcement capacity building, establishing dedicated victim rehabilitation centers, and formulating robust frameworks for victim compensation.

21. **Smt. Vijaya Bharathi Sayani, Hon'ble Member, NHRC** stressed that protecting citizens' life, dignity, and property is a fundamental State responsibility, and that safeguarding them from cybercrime and financial fraud is an essential extension of good governance in the digital era, requiring not just technological and regulatory measures but effective governance and collective action.

22. **Dr Justice Bidyut Ranjan Sarangi, Hon'ble Member, NHRC** appreciated the rich deliberations and diverse perspectives shared during the discussion. He noted that technological advancement inevitably brings new challenges, but collective efforts and stakeholder feedback would help identify solutions and address gaps. He stressed the need to develop practical recommendations to help institutions respond effectively to emerging cyber threats.

23. In his concluding remarks, **Justice V. Ramasubramanian, Hon'ble Chairperson, NHRC,** noted that prevented frauds far outnumber successful ones, though they go largely unnoticed compared to crimes that make headlines. As the Commission is not a technical body, he asked stakeholders to flag specific legal loopholes. He noted that limited access to service-provider information sometimes hampers action against cybercrime, and suggested exploring alert systems during prolonged suspicious calls, including on OTT platforms, to warn users of possible digital arrest scams. He observed that fraud constantly evolves as criminals adapt to countermeasures, and that full citizen preparedness may not be achievable despite awareness efforts. He supported the idea of forming thematic sub-committees and stressed that those combating cybercrime must collaborate as a network, just as fraudsters do.

24. The discussion ended with a vote of thanks to the Chair and other participants present.

Annex

List of Participants

NHRC Officials

1. Justice V. Ramasubramanian, Hon'ble Chairperson
2. Justice (Dr.) Bidyut Ranjan Sarangi, Hon'ble Member
3. Smt. Vijaya Bharathi Sayani, Hon'ble Member
4. Shri Bharat Lal, Secretary General
5. Ms. Anupama Nilekar Chandra, Director General (Investigation)
6. Shri Samir Kumar, Joint Secretary
7. Ms. Saidingpuii Chhakchhuak, Joint Secretary
8. Dr. Rajul Raikwar, Consultant (Research)
9. Ms. Lakshmi Kumari, JRC

Invitees

10. Shri Ajit Kumar, Joint Secretary, Ministry of Electronics and Information Technology
11. Shri Sanjeev Kumar Sharma, Deputy Director General (AI & Digital Intelligence Unit), Department of Telecommunications
12. Shri Ashok Kumar, Joint Advisor, Telecom Regulatory Authority of India (TRAI)
13. Shri R Vanaraja, Chief General Manager, Department of Information Technology, Reserve Bank of India
14. Shri Brijesh Singh, ADG, Maharashtra
15. Smt Roopa M, Inspector General of Police, Indian Cyber Crime Coordination Centre (I4C)
16. Ms. Astha Modi, SP, Cyber Division, Central Bureau of Investigation
17. Dr. Muktesh Chander, NHRC Special Monitor, Cybercrime and Artificial Intelligence
18. Shri Ramesh Krishnamoorthy, Chief Risk Management, National Payments Corporation of India
19. Shri Rahul Vatts, Chief Regulatory Officer, Airtel
20. Shri Rajeev Prasad, Senior Advisor, Payments Systems & Banking Technology, Indian Banks' Association
21. Ms. N.S. Nappinai, Senior Advocate, Supreme Court
22. Dr. Pavan Duggal, Advocate, Supreme Court of India
23. Maj Vineet Kumar, Founder & Global President, CyberPeace Foundation

***

The suggestions emanated from the NHRC Open House Discussion '*Safeguarding Human Rights against Digital Arrest Scams*', are as follows:

I. **Legal and Regulatory reform**

i.) Digital arrest Scams should be made a distinct offence under the IT Act, 2000 or the Bharatiya Nyaya Sanhita, 2023, to enable registration of cases under a specific section and ensure stronger deterrence.

ii.) Renting, sale, and opening of mule accounts should be criminalised through a statutory provision.

iii.) A statutory framework may be created to enable real-time suspension of accounts exhibiting suspicious activity.

iv.) Banks' intermediary obligations should be clearly defined under Section 2(1)(w) of the IT Act through rules under Section 87(2), linked to their existing due-diligence duties under Section 79(2)(c), so that banks cannot claim ignorance of fraudulent fund transfers.

v.) Adjudicatory mechanisms under Section 46 of the IT Act should be strengthened, and faster convictions pursued under existing provisions such as extortion and Section 66D.

vi.) All intermediaries operating in India should be required to maintain accessible nodal officer contacts for law enforcement agencies.

vii.) OTT communication platforms and messaging apps should be brought under telecom-grade statutory regulation through a unified national framework, as fraud is increasingly migrating from telecom channels to these largely unregulated platforms.

viii.) The Digital Personal Data Protection Act and its Rules should be fully and timely implemented to strengthen intermediary accountability, enforce dual account detection, and reduce data vulnerabilities that cybercriminals exploit. Further, the authorities may consider developing a proportionate AI framework.

II. **Institutional and Enforcement Reforms**

i.) A National Cybercrime Force with end-to-end, real-time operational visibility across cybercrime incidents should be established.

ii.) Cases exceeding a prescribed financial threshold should be automatically diverted to a central investigating body given the transnational and complex nature of such crimes.

iii.) An automated Golden Hour Protocol should be put in place to speed up fund tracing and intervention immediately after a fraud is reported.

iv.) Automatic conversion of complaints into FIRs upon fulfilment of sufficient evidentiary criteria should be mandated, reducing discretion and the associated risk of corruption.

v.) SIM card issuance should be regulated with the same rigour as other controlled items. Strict telecom KYC compliance should be enforced and misuse of SIM boxes and bulk SIM issuance by syndicates should be curbed.

III. **Financial Safeguards and Victim Compensation**

i.) A statutory circuit-breaker mechanism may be considered for banks to delay transfers above a prescribed limit by 2–3 hours. A similar delayed credit window can be introduced for RTGS and NEFT settlements at the customer transaction phase, before interbank settlement is completed.

ii.) A victim-centric compensation framework based on restorative justice principles should be developed, ensuring timely payouts even where individual liability is difficult to establish.

iii.) A shared liability model should be built involving banks, telecom providers, SIM-issuing points of sale, and payment intermediaries, drawing on international collective-accountability frameworks such as the Authorised Push Payment model, to enable recovery of defrauded amounts.

iv.) A Digital Arrest Victims Fund, financed by stakeholders in the transfer chain, should be established, with non-compliant banks losing their safe-harbour exemption under Section 79 of the IT Act.

v.) A uniform, nationwide mechanism for restoration of defrauded funds should be developed, building on the Standard Operating Procedure already formulated by I4C and MHA.

IV. **Technology, Detection, and Prevention**

i.) Scale up the Mule Hunter Programme and share red-flag indicators across banks, telecom operators, payment providers, and digital platforms.

ii.) Consider automated intervention mechanisms like kill switch to detect and disrupt prolonged coercive audio-video sessions on OTT platforms used in digital arrest scams, breaking the psychological hold fraudsters maintain over victims and allowing family members or actual police to intervene.

iii.) Digitise government notice and summons processes and provide a centralised verification portal for citizens, eliminating impersonation using fabricated official documents.

iv.) Develop a comprehensive, AI-enabled national database of digital arrest cases for pattern recognition, predictive analysis, and proactive prevention.

v.) Extend fraud-monitoring and intervention capabilities to OTT and digital communication platforms.

V. **Reporting Accessibility and Public Awareness**

i.) Make the 1930 helpline and cybercrime.gov.in portal multilingual and equipped with AI-powered chatbot support to improve accessibility for rural populations, farmers, senior citizens, and individuals with limited digital literacy.

ii.) Continue and intensify multi-channel public awareness campaigns, focusing on scam recognition, safe disengagement techniques, and prompt reporting.

VI. **Victim Support, Rehabilitation, and Psychological Care**

i.) The narrative must shift from victim-blaming to recognising digital arrest as a violation of fundamental rights under Article 21. Victims suffer lifelong stigma, psychological trauma, and invasion of dignity that must be formally acknowledged.

ii.) Victim-focused psychological support programmes such as the Cyber Heal initiative with NIMHANS should be expanded. These should be institutionalised as part of a broader framework integrating legal redressal and financial compensation.

iii.) Specialised cyber rehabilitation centres should be established for offenders, particularly juveniles and first-time offenders, offering psychometric assessment and structured rehabilitation rather than routing them through standard juvenile homes or detention facilities.

VII. **Recommendations for NHRC**

i.) Constitute a high-level expert panel to specifically examine the human rights implications of digital arrest scams.

ii.) Establish specialised thematic sub-committees to address legal reforms, real-time inter-agency coordination, victim compensation, and accountability frameworks.

iii.) Consider taking cognisance of such serious cybercrime complaints and monitor state responses relating to FIR registration, investigation, and recovery efforts.

***