Cybercrime Update

'Police' and 'Public Order' are State subjects under the seventh schedule of the Constitution of India. Accordingly, States and Union Territories (UTs) are primarily responsible for preventing, detecting, investigating, and prosecuting crimes, including cybercrimes and digital arrest scams, through their Law Enforcement Agencies (LEAs). The central government supports these efforts by issuing advisories and providing financial assistance under various schemes to build the capacity of LEAs.

The National Crime Records Bureau (NCRB) compiles and publishes crime statistics in its annual report, *Crime in India*, with the latest available data

for 2022. However, NCRB does not maintain specific data on digital arrest scams separately.

Steps Taken by the Central Government

To strengthen the mechanism to deal with cyber crimes including digital arrest scams in a comprehensive and coordinated manner, the central government has taken steps which, inter-alia, include the following:

i. The Ministry of Home Affairs has set up the 'Indian Cyber Crime Coordination Centre' (I4C) as an attached office to deal with all types of cybercrimes in the country, in a coordinated and comprehensive manner.
ii. The central government has launched a comprehensive awareness program on digital arrest scams which, inter-alia, includes; newspaper advertisements, announcements in Delhi Metros, use of social media influencers to create special posts, campaign through Prasar Bharti and electronic media, a special program on Aakashvani and participated in Raahgiri Function at Connaught Place, New Delhi on 27.11.2024.
iii. I4C proactively identified and blocked more than 1700 Skype IDs and 59,000 Whatsapp accounts used for digital arrest.
iv. The central government has published a press release on alert against incidents of 'Blackmail' and 'Digital Arrest' by cyber criminals impersonating State/UT Police, NCB, CBI, RBI, and other law enforcement agencies.
v. The central government is collaborating with Telecom Service Providers (TSPs) to block incoming international spoofed calls

that display Indian mobile numbers, targeting scams such as fake digital arrests, FedEx frauds, and impersonation of government and police officials.

vi. Till 15.11.2024, the Government of India has blocked more than 6.69 lakhs SIM cards and 1,32,000 IMEIs as reported by the police authorities.

vii. Launching the National Cyber Crime Reporting Portal (https://cybercrime.gov.in) under I4C to facilitate the public reporting of cybercrimes, with a focus on crimes against women and children. State/UT LEAs address the cases that public report reported on this portal as per the law.

viii. Introducing the 'Citizen Financial Cyber Fraud Reporting and Management System' in 2021 to enable immediate reporting of financial frauds and prevent fund diversion. To date, over ₹3,431 crore has been recovered from more than 9.94 lakh complaints. The toll-free helpline number '1930' has been operationalized for lodging cyber complaints.

ix. To spread awareness of cybercrime, the central government has taken steps which, inter-alia, include the following:

- Disseminating messages through SMS, I4C social media accounts i.e. X (formerly Twitter) (@CyberDost), Facebook(CyberDostI4C), Instagram (cyberDostI4C), Telegram(cyberdosti4c)

- Radio campaign, engaged MyGov for publicity in multiple mediums

- Organizing Cyber Safety and Security Awareness weeks in association with States/UTs,
- Publishing a handbook for adolescents/students, digital displays on railway stations and airports and other public spaces.

References

http://www.pib.gov.in/Pressreleaseshare.aspx?PRID=2082761