

**GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS**

**RAJYA SABHA
UNSTARRED QUESTION NO. 2788**

TO BE ANSWERED ON THE 12TH AUGUST, 2026/ SHRAVANA 21, 1948 (SAKA)

CYBER FRAUDSTERS EMPTYING BANK ACCOUNTS BY SENDING FAKE E-CHALLANS

2788 # SHRI NEERAJ DANGI:

Will the Minister of Home Affairs be pleased to state:

(a) whether Government is aware of the increasing incidents of cyber fraudsters emptying bank accounts by sending fake e-challans;

(b) the number of such cases registered in the last two years, the amount that has been scammed, the number of cases resolved and the detail of action taken against the culprits;

(c) the special training and resources being provided by Government to State police and cyber cells for the investigation of such cybercrimes; and

(d) whether Government is operating any time-bound mechanism to assist victims of such cyber frauds in swift recovery of funds, if so, the details thereof?

ANSWER

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS

(SHRI BANDI SANJAY KUMAR)

(a) to (d) : The National Crime Records Bureau (NCRB) compiles and publishes the statistical data on crimes in its publication “Crime in India”.

The latest published report is for the year 2024. Data regarding cases registered, cases resolved and the amount scammed in fake e-challans is not maintained by NCRB.

The ‘Citizen Financial Cyber Fraud Reporting and Management System’ (CFCFRMS), under Indian Cyber Crime Coordination Centre (I4C), has been launched in year 2021 for immediate reporting of financial frauds and to stop siphoning off funds by the fraudsters. As per CFCFRMS operated by I4C, till 30.06.2026, financial amount of more than Rs. 11,158 Crore has been saved in more than 32.80 lakh complaints.

‘Sahyog’ Portal has been launched to expedite the process of sending notices to IT intermediaries by the Appropriate Government or its agency under clause (b) of sub-section (3) of section 79 of the IT Act, 2000 to facilitate the removal or disabling of access to any information, data or communication link being used to commit an unlawful act. I4C has blocked more than 2,77,053 illegal and fraudulent Apps/ content/ websites/ E-mail Accounts/ URLs/ Links across various platforms through Sahyog portal and proactive action by informing concerned IT intermediaries.

‘Police’ and ‘Public Order’ are State subjects under the Seventh Schedule to the Constitution of India. Accordingly, the States and Union Territories (UTs) are primarily responsible for the prevention, detection, investigation, and prosecution of cybercrime. The Central Government,

through the Ministry of Home Affairs (MHA), supplements the efforts of States and UTs by providing policy guidance, technological support, capacity-building assistance, and financial resources to strengthen cybercrime management and enforcement capabilities.

The Massive Open Online Courses (MOOC) platform, namely 'CyTrain' portal has been developed under I4C, for capacity building of police officers/judicial officers through online course on critical aspects of cyber crime investigation, forensics, prosecution etc. Till 30.06.2026, more than 1,63,344 police officers/judicial officers from States/UTs are registered and more than 1,61,957 Certificates issued through the portal.

Cyber Commando programme was launched by the Hon'ble Home Minister on 10.09.2024 to establish a Special Wing of Cyber Commandos equipped with specialized training to counter cybersecurity threats in the country. The programme envisions the creation of a dedicated, skilled workforce capable of securing critical information infrastructure and supporting national cybersecurity efforts. 281 cyber commandos successfully completed training.

I4C, MHA is regularly organising ‘State Connect’, ‘Thana Connect’ ‘Bank Connect’ and Peer learning session to share best practices, enhance capacity building, etc.

The state of the art National-Digital Investigation Support Centre (previously known as National Cyber Forensic Laboratory (Investigation) {NCFL(I)}) has been established, as a part of the I4C, at New Delhi (on 18.02.2019) and at Assam (on 29.08.2025) to provide early stage cyber forensic assistance to Investigating Officers (IOs) of State/UT Police. Till 30.06.2026, National-Digital Investigation Support Centre, New Delhi has provided its services to State/UT LEAs in more than 14,064 cases pertaining to cyber crimes.

To further strengthen operational efficiency and ensure uniformity in handling cybercrime complaints, the Ministry has issued a comprehensive Standard Operating Procedure (SOP) for NCRP-CFCFRMS. The SOP lays down a standardized framework for complaint processing, bank coordination, grievance redressal, removal of lien markings, and restoration of defrauded funds to rightful claimants based on complaints received through the NCRP. Money Restoration Module for expeditious restoration of defrauded money to the victims and Grievance Redressal Module for timely attending to the grievances relating to freezing of the bank accounts and lien marking of the amount, have been made functional from April, 2026.