

**GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS**

**LOK SABHA
UNSTARRED QUESTION NO. 1603**

TO BE ANSWERED ON THE 28TH JULY, 2026/ SHRAVANA 6, 1948 (SAKA)

CYBER CRIME REPORTING PORTAL

**1603. DR. D RAVI KUMAR:
SHRI RAJIV PRATAP RUDY:
SHRI AZAD KIRTI JHA:**

Will the Minister of HOME AFFAIRS be pleased to state:

(a) whether the Government is aware that State Police, including Tamil Nadu Police are heavily dependent on the National Cyber Crime Reporting Portal (NCRP) and the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) for freezing and recovering money lost in cyber frauds;

(b) the total number of cybercrime complaints and financial fraud cases registered on the NCRP during the last three years, State/UT and category-wise along with the financial losses reported by citizens due to online scams and the quantum of funds successfully saved or frozen through CFCFRMS;

(c) the number of mule bank accounts, suspicious SIM cards, international mobile equipment identities (IMEIs) identified and blocked through coordination with financial institutions and telecom service providers along with the standard operating procedures (SOPs) issued to state law enforcement agencies to handle cyber fraud;

(d) whether it is a fact that the sharp rise in cyber fraud complaints involving thousands of crores of rupees has led to delays in freezing fraudulent transactions and refunding victims along with the number of complaints received, amount frozen and amount refunded through the Portal, State-wise, during 2024-25 and 2025-26; and

(e) whether the Government has any proposal to strengthen staffing, banking coordination and technical support provided to States for cyber crime prevention to ensure quicker recovery and refund of defrauded amounts and if so, the details thereof?

ANSWER

**MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS
(SHRI BANDI SANJAY KUMAR)**

(a) to (e) : ‘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 Ministry of Home Affairs has set up the ‘Indian Cyber Crime Coordination Centre’ (I4C) as an attached office to deal with all types of cyber crimes in the country, in a coordinated and comprehensive manner.

The ‘National Cyber Crime Reporting Portal’ (NCRP) (<https://cybercrime.gov.in>) has been launched, as a part of the I4C, to enable public to report incidents pertaining to all types of cyber crimes, with special focus on cyber crimes against women and children.

The ‘Citizen Financial Cyber Fraud Reporting and Management System’ (CFCFRMS), under 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. As per NCRP & CFCFRMS operated by I4C, during the year 2023 to 2025, the total number of cyber fraud complaints on NCRP are more than 50,11,083 the total amount marked as Lien is more than ₹ 7,788 crores, and the amount refunded is more than ₹ 132 crores.

A Suspect Registry of identifiers of cyber criminals has been launched by I4C on 10.09.2024 in collaboration with Banks/Financial Institutions. Till 30.06.2026, more than 30.48 lakh suspect identifier data received from Banks and 32.08 lakh Layer 1 mule accounts have been shared with the participating entities of Suspect Registry and declined transactions worth Rs. 25,698 crores. Till 30.06.2026, more than 15.75 lakhs SIM cards and 5.77 lakhs IMEIs as reported by Police authorities have been blocked by Government of India.

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.

I4C, MHA is regularly organising 'State Connect', 'Thana Connect', 'Bank Connect' and peer learning sessions to share best practices, enhance capacity building, etc.

*** * * * ***