

CYBERCRIME PROCEEDS LINKED TO MONEY LAUNDERING NETWORKS

Posted On: 24 MAR 2026 4:20PM by PIB Delhi

As per Directorate of Enforcement (ED), till 28.02.2026, the Directorate has taken up around 257 cases related to cybercrime for investigation under the provisions of Prevention of Money Laundering Act, 2002 (PMLA), resulting in identification of Proceeds of Crime (PoC) worth 35,925.58 crore rupees. The data regarding scale of cybercrime proceeds, State-wise is not maintained by ED.

There is an established mechanism for sharing/ dissemination of information between the Directorate of Enforcement and other Law Enforcement Agencies (LEA) through respective Nodal Officers. Under this mechanism, ED and LEAs share information including matters related to cybercrime. In addition, the Directorate shares information with other agencies under section 66(2) of PMLA, whenever, a contravention pertaining to the relevant agency is noticed during investigation under PMLA.

ED is also using SAHYOG, Samanvaya and Cyber Police Portal maintained by Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs (MHA). Further, the Directorate also use the Inter-operable Criminal Justice System (ICJS) portal accessing the FIRs registered by various State Police related to Cybercrimes.

‘Police’ and ‘Public Order’ are State subjects as per the Seventh Schedule of the Constitution of India. The States/UTs are primarily responsible for the prevention, detection, investigation, complaint reporting, recovery actions, victim support systems, prosecution of crimes including cyber fraud through their Law Enforcement Agencies (LEAs). The Central Government supplements the initiatives of the States/UTs through advisories and financial assistance under various schemes for capacity building of their LEAs.

To strengthen the mechanism to deal with cyber crimes including detection and recovery of funds siphoned through digital and online fraud networks in a comprehensive and coordinated manner, the Central Government has taken steps which, inter-alia, include the following:

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. Cyber crime incidents reported on National Cyber Crime Reporting Portal, their conversion into FIRs and subsequent action i.e. filing of chargesheets, arrest and resolution of complaints, thereon are handled by the State/UT Law Enforcement Agencies concerned as per the provisions of the law.

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 31.01.2026, financial amount of more than Rs.

8,690 Crore has been saved in more than 24.65 lakh complaints. A toll-free Helpline number '1930' has been operationalized to get assistance in lodging online cyber complaints.

A State of the Art, Cyber Fraud Mitigation Centre (CFMC) has been established at I4C where representatives of major banks, Financial Intermediaries, Payment Aggregators, Telecom Service Providers, IT Intermediaries and representatives of States/UTs Law Enforcement Agency are working together for immediate action and seamless cooperation to tackle cybercrime.

A Suspect Registry of identifiers of cyber criminals has been launched by I4C on 10.09.2024 in collaboration with Banks/Financial Institutions. Till 31.01.2026, more than 23.05 lakh suspect identifier data received from Banks and 27.37 lakh Layer 1 mule accounts have been shared with the participating entities of Suspect Registry and declined transactions worth Rs. 9518.91 crores.

Samanvaya Platform has been made operational to serve as an Management Information System (MIS) platform, data repository and a coordination platform for LEAs for cybercrime data sharing and analytics. It provides analytics based interstate linkages of crimes and criminals, involved in cybercrime complaints in various States/UTs. The module 'Pratibimb' maps locations of criminals and crime infrastructure on a map to give visibility to jurisdictional officers. The module also facilitates seeking and receiving of techno-legal assistance by Law Enforcement Agencies from I4C and other SMEs. It has lead to arrest of more than 21,857 accused and more than 1,49,636 Cyber Investigation assistance request.

A comprehensive Standard Operating Procedure (SOP) has been issued by the Central Government on 2nd January 2026. It provides a uniform, victim-centric framework for handling complaints through the National Cybercrime Reporting Portal (NCRP) and Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS). The Standard Operating Procedure (SOP) for NCRP-CFCFRMS outlines a dedicated Coordination Mechanism to enhance collaboration, particularly with States and Union Territories, whose police agencies are integral stakeholders in the system.

This was stated by the Minister of State in the Ministry of Home Affairs Shri Bandi Sanjay Kumar in a written reply to a question in the Lok Sabha.

RK/RR/PR/PS/AG

(Release ID: 2244499) Visitor Counter : 142

Read this release in: Urdu , हिन्दी