



CYBER CRIME VICTIM ASSISTANCE AND FRAUDULENT AMOUNT RECOVERY SCHEME, 2026

**(In pursuance of the directions of the Hon'ble Supreme Court of
India in Suo Motu Writ Petition (Criminal) No. 3 of 2025)**

CHHATTISGARH STATE LEGAL SERVICES AUTHORITY

CYBER CRIME VICTIM ASSISTANCE AND FRAUDULENT AMOUNT RECOVERY SCHEME, 2026

Table of Contents

1. Introduction.....	3
2. Name of Scheme.....	5
3. Definitions.....	5
4. Objectives of the Scheme.....	6
5. Beneficiaries of the Scheme.....	6
6. Assistance under the Scheme.....	6
7. Assistance in Freezing/Holding the Amount/Account.....	7
8. Which kind of Legal Assistance to be provided.....	8
9. Special Cyber Legal Assistance Cell.....	8
10. Timeline.....	9
11. Cases Requiring Special Priority.....	9
12. Public Awareness Programmes.....	9
13. Role of PLVs.....	10
14. Coordination with Banking Institutions.....	10
15. Financial Provisions.....	10
16. Institutional Responsibilities.....	11
17. Complaint Form (Annexure-A).....	12
18. Monitoring/Surveillance-MIS (Annexure-B).....	13
19. Standard Operating Procedure (SOP) for Cyber Victim Assistance (Annexure-C).....	14

CYBER CRIME VICTIM ASSISTANCE AND FRAUDULENT AMOUNT RECOVERY SCHEME, 2026

1. Introduction

The rapid expansion of digital technology, internet services, and online financial transactions has significantly transformed the way people access banking, payments, shopping, investments, communication, and various government and non-government services. While digitalisation has made services faster, more convenient, and accessible, the increasing dependence on digital platforms has also resulted in a growing risk of cybercrime, particularly cyber fraud.

Cybercrime refers to offences in which computers, mobile phones, the internet, digital networks, or other information and communication technologies are used to commit an offence, cause harm to an individual or organisation, obtain unlawful financial gain, or illegally access or misuse personal or confidential information. Cybercrime covers a wide range of offences, including website hacking, cyber stalking, software piracy, virus attack, phishing, illegal sale of goods, email spoofing, online gambling, cyber defamation, counterfeiting (forgery), email bombing, e-commerce/investment fraud, OTP (one time password), misuse of photocopies of Identity cards, credit/debit card skimming, AI-based cybercrimes, ransomware attacks, digital arrest, pornography, unauthorised access, data theft, identity theft, online harassment, and various forms of online financial fraud.

Among these, **cyber fraud** has emerged as one of the most serious and rapidly evolving forms of cybercrime. Cyber fraud involves the use of digital means to deceive individuals or organisations with the intention of obtaining money, financial credentials, personal information, or other valuable data. Common forms of cyber fraud include **phishing, fraudulent banking calls and links, UPI and online banking fraud, credit/debit card fraud, fake shopping websites, identity theft, investment fraud, digital arrest scams, and other forms of online financial fraud**. In many such cases, fraudsters exploit trust, fear, greed, or a sense of urgency to induce victims to disclose sensitive information or transfer money themselves.

The increasing volume of digital transactions has also been accompanied by substantial financial losses arising from cyber fraud. As per the data reported by the **Press Information Bureau (PIB)**, the amount of money lost in cyber fraud cases has been significant in recent years:

Year	Lost Money
2023	₹7,463 crore lost.
2024	₹22,849 crore lost.
2025	₹19,812 crore lost

These figures demonstrate that cyber fraud is no longer merely a technological concern; it has become a serious economic, social, and legal challenge affecting individuals, families, businesses, and society at large. The nature of digital financial fraud is such that the proceeds of fraud may be rapidly transferred through multiple bank accounts, payment platforms, or other digital channels. Consequently, any delay in reporting the incident and immediately informing the concerned bank or financial institution may reduce the possibility of stopping further transfers and recovering the defrauded amount.

In such circumstances, victims of cyber fraud require not only assistance from the police and banking institutions but also timely legal assistance, proper guidance, facilitation, and coordination with the concerned authorities and departments. This becomes particularly important for persons who are vulnerable, economically weaker, or otherwise unable to effectively pursue available legal remedies on their own.

NALSA is presently implementing various preventive and strategic legal services schemes. In compliance with Paragraph 7(VII) of the order dated 04.08.2026 passed by the Hon'ble Supreme Court in ***SUO MOTU WRIT PETITION (CRIMINAL) NO. 03/2025, In Re: Victims of Digital Arrest Related to Forged Documents***, and keeping in view the role of Legal Services Authorities in implementing preventive and strategic legal services schemes, this scheme is proposed to provide immediate legal assistance, guidance, and coordination with concerned departments to victims of cybercrime.

2. Name of the Scheme

Cyber Crime Victim Assistance and Fraudulent Amount Recovery Scheme, 2026

3. Definitions

Unless otherwise required by the context in this scheme

1. **“Act”** refers to the Legal Services Authorities Act, 1987 (Act No. 39 of 1987)
2. **“Cybercrime”** refers to any online crime committed using the internet or digital devices including online fraud, theft, espionage, viruses attack and other offenses.
3. **“Intermediary”**, with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes.
4. **“Legal services”** shall have the same meaning as defined under Section 2(c) of the Legal Services Authorities Act, 1987.
5. **“Legal service clinic”** refers to a clinic as defined under Regulation of the National Legal Services Authority (Legal Services Clinics) Regulations, 2011.
6. **“Legal service institution”** refers to the State Legal Services Authority, Supreme Court Legal Services Committee, High Court Legal Services Committee, District Legal Services Authority, or Taluka Legal Services Committee, as applicable.
7. **“Panel Lawyer”** refers to those panel lawyers selected under Regulation 8 of the National Legal Services Authority (Free and Competent Legal Services) Regulations, 2010.
8. **“Para-Legal Volunteer”** refers to individuals defined as Para-Legal Volunteers (Adhikar Mitra) under the NALSA Para-legal Volunteers Scheme (Revised) Para-Legal Volunteers Training Module.
9. All other terms and expressions used in this scheme but not specifically defined shall carry the same meaning as assigned to them under the Legal Services Authorities Act 1987 (Act No. 39 of 1987), the National Legal Services Authority Rules, 1995, or the National Legal Services Authority (Free und Competent Legal Services) Regulations 2010, as applicable.

4. Objectives of the Scheme

The objectives of this Scheme shall be:

1. To provide prompt and effective legal assistance to persons affected by cybercrime/cyber fraud.
2. To assist in immediately communicating information regarding cyber financial fraud to the concerned Police/Cyber Cell and bank.
3. To assist victims in the process of getting the defrauded amount frozen/put on hold.
4. To assist in the recovery/return of the amount that has been frozen/put on hold through legal proceedings.
5. To guide victims regarding necessary action before the bank, police, Cyber Cell, and courts.
6. To create widespread public awareness regarding cybercrimes with a view to preventing such offences.
7. To provide special assistance to senior citizens, women, persons with disabilities, and economically weaker persons.
8. To develop an effective coordination mechanism among SLSA, DLSA, Police, Cyber Cell, and banking institutions.

5. Beneficiaries of the Scheme

The following persons shall be eligible to receive assistance under the Scheme:

- Persons who are victims of cybercrime/online financial fraud.
- Persons whose bank accounts have been subjected to unauthorized transactions through UPI, debit/credit cards, wallets, or other digital payment modes.
- Persons who have lodged a cybercrime complaint by calling **1930** or through the **National Cyber Crime Reporting Portal**.
- Eligible persons who are entitled to receive free legal services.

6. Assistance under the Scheme

DLSA/PLV shall provide the following assistance to the victim:

A. Immediate Assistance

- Assistance in lodging a complaint on **1930**.

- Assistance in lodging a complaint on the **National Cyber Crime Reporting Portal**.
- Assistance in immediately informing the concerned bank/Intermediary.
- Assistance in collecting the details of the relevant transaction.
- Assistance in safely preserving necessary details such as UTR/Transaction ID, account number, mobile number, etc.
- Assistance in submitting a complaint before the Police/Cyber Cell.

B. Assistance in Preserving Digital Evidence

- Assistance in preserving screenshots of suspicious messages, WhatsApp chats, call recordings, email headers, and links.
- Assistance in obtaining bank passbook/statements, UPI reference numbers (UTR), and payment gateway receipts.
- Assistance in collecting details of APK files used in the fraud, phishing links, or remote-access applications such as AnyDesk, TeamViewer, etc.

7. Assistance in Freezing/Holding the Amount/Account

The **Cyber Legal Assistance Coordinator**, appointed by the DLSA, who may be a suitable person or PLV as determined by the DLSA for this purpose, shall ensure that necessary coordination takes place between the victim, Cyber Police, and the concerned bank/financial institution.

Where the amount has already been transferred to other accounts, the victim shall be assisted in identifying the concerned accounts and taking necessary action in accordance with the legal procedure available through the Police/Cyber Cell.

Clarification: DLSA itself shall not issue any order to freeze or unfreeze any bank account. Such action shall be taken by the competent Police/Investigating Officer, bank, or competent court in accordance with the applicable law.

8. Which kind of Legal Assistance to be provided

Eligible persons, under the **Legal Services Authorities Act, 1987**, may be provided free legal assistance for the following purposes:

- Filing an application before the Police.
- Making a representation before the Cyber Cell.
- Making a representation before the bank/financial institution.
- Preparation of necessary affidavits/applications.
- Filing necessary applications before the court.
- Providing legal advice regarding available legal remedies for release/recovery of the frozen amount.
- Filing and pursuing an application before the Magistrate Court for release/return of the frozen amount in favour of the victim under **Section 503 of the BNSS (Bharatiya Nagarik Suraksha Sanhita) / Section 457 of the Code of Criminal Procedure, 1973** as applicable.

Note- If a person is not otherwise, eligible in under section 12 of legal services authority act 1987 the assistance may be provided through pro bono lawyers.

9. Special Cyber Legal Assistance Cell

A Cyber Legal Assistance Cell (CLAC) shall be established in every DLSA.

Composition of the Cell

Position/Person	Role
Secretary, District Legal Services Authority (DLSA)/Nodal Officer	Overall supervision
Panel Advocate	Legal assistance
PLV	Victim contact and awareness
Cyber Police Officer	Police coordination
Bank Nodal Officer	Banking-related coordination
Data Entry/Support Staff	Records and MIS

10. Timeline

Time	Proposed Action
0–2 hours	Information to 1930/Bank/Cyber Portal
Within 24 hours	Preliminary legal assistance
Within 48 hours	Initial status from Cyber Cell/Bank
7 days	Review of status of freezing/tracing
15 days	Review of pending cases
Every month	DLSA to submit MIS report to SLSA

Note: The internal advisory timelines of the DLSA shall be applicable only for internal coordination and shall not be treated as timelines applicable to the actions of the Police/Bank.

11. Cases Requiring Special Priority

The following cases shall be given priority:

- Senior citizens.
- Women.
- Persons with disabilities.
- Adolescents/children involved in cases relating to financial fraud.
- Economically weaker persons.
- Fraud involving a large amount.
- Complaints received immediately after the incident.
- All other cases where there is a possibility of recovery of the defrauded amount.

12. Public Awareness Programmes

SLSA/DLSA may organise public awareness campaigns in collaboration with government and non-government departments to aware and educate the general public, children, women, and senior citizen about cyber security, cybercrime, cyber fraud and how to prevent them at the following places:

- Schools/colleges.
- Court premises.
- Gram Panchayats.

- Janpad Panchayats.
- Urban local bodies.
- Old-age homes.
- Legal awareness camps.
- Banks and Common Service Centres.

13. Role of PLVs

PLVs shall be specially trained to:

1. Identify cyber fraud.
2. Inform victims about 1930.
3. Connect victims with the DLSA.
4. Follow up on the status of complaints.
5. Organize extensive awareness programmes for prevention of cyber fraud.
6. Provide special assistance to categories of persons eligible to receive legal assistance under this Scheme.

14. Coordination with Banking Institutions

At the DLSA level, coordination may be established with major banks, Banking Ombudsman/LBD (Lead Bank), and other relevant banking institutions.

In each district, the concerned banking institutions may be requested to nominate a Nodal Officer.

This shall facilitate a prompt coordination mechanism among:

DLSA ↔ Cyber Police ↔ Bank Nodal Officer

15. Financial Provisions

For the Scheme, expenditure may be provided from the NALSA funds made available to the SLSA under the following heads:

1. Expenditure towards publicity, dissemination, and awareness.
2. Training programmes for concerned personnel/stakeholders.
3. Expenses for meetings of the Cyber Legal Assistance Cell.
4. Honorarium/remuneration for PLVs/legal assistance and Panel Advocates.

The SLSA shall **not automatically compensate/reimburse the defrauded amount**.

Recovery/refund of the amount shall be made in accordance with the applicable law, banking regulations, and the orders of the competent authority/court.

16. Institutional Responsibilities

SLSA

- State-level supervision of the Scheme.
- Issuance of SOP.
- Collection of monthly MIS from DLSAs.
- State-level coordination with Police/Cyber Cell/Banking authorities.
- Conducting training and awareness programmes.

DLSA

- Operation of the Cyber Legal Assistance Cell.
- Providing legal assistance to victims.
- Coordination with Cyber Cell and banks.
- Monitoring cases.
- Sending monthly information to the SLSA.
-

Panel Advocate

- Providing legal advice to victims on the direction of the DLSA.
- Preparing necessary applications.
- Representing victims in judicial proceedings.

PLV

- Providing initial assistance.
- Creating awareness.
- Connecting victims with the DLSA.
- Undertaking follow-up action.

Police/Cyber Cell

- Investigation of the offence.
- Tracing transactions.

- Taking necessary freezing/holding action.
- Investigation/inquiry and recovery in accordance with applicable law.

Complaint Form

CYBER CRIME VICTIM ASSISTANCE FORM

- Name:
- Address:
- Mobile Number:
- Date of Incident:
- Time of Incident:
- Amount of Fraud:
- Mode: UPI/Bank/Card/Wallet/Other.....
- Transaction ID/UTR:
- Bank Name:
- 1930 Complaint No.:
- Cyber Portal Complaint No.:
- FIR/Police Complaint No.:
- Amount Frozen:
- Amount Recovered:
- Present Status:
- Legal Assistance Required: Yes/No.....

Monitoring/Surveillance – MIS

Each DLSA shall send the following information to the SLSA on a monthly basis:

- Serial number/details and amount.
- Complaints received.
- Victims provided legal assistance.
- Total amount defrauded:
- Cases reported on 1930.
- Amount frozen/put on hold:
- Amount recovered:
- Pending cases.
- Disposed cases.
- Awareness programmes conducted.
- Number of beneficiaries.

Standard Operating Procedure (SOP) for Cyber Victim Assistance

Step 1 – Receipt of Complaint

The victim shall contact the DLSA/Front Office/PLV.

Step 2 – Immediate Alert

The victim shall be advised to **call 1930 immediately after the cyber fraud occurs.**

Step 3 – Verification of Complaint

The following information shall be collected:

- Name and contact details of the victim.
- Date and time of the incident.
- Amount defrauded.
- Transaction ID/UTR.
- Bank/UPI/wallet details.
- Complaint number received after reporting on 1930.
- Complaint number received after reporting on the Cyber Crime Portal.
- Police complaint/FIR number, if available.

Step 4 – Intimation to Bank

The victim shall be assisted in immediately reporting the fraud to the concerned bank/financial institution/Intermediary.

Step 5 – Cyber Police Coordination

The Nodal Officer of the DLSA shall coordinate with the concerned officer of the Cyber Cell.

Step 6 – Tracing/Freezing of Amount

Where possible, action shall be taken by the competent agency for putting the amount on hold/freezing the amount.

Step 7 – Legal Assistance

Where judicial proceedings are required, an eligible victim shall be provided a Panel Advocate.

Step 8 – Follow-up Action

The DLSA shall periodically review the status of each case. Once the amount is recovered or all available legal remedies have been exhausted, the case shall be recorded as **closed/disposed of**.

•

CYBER CRIME VICTIM ASSISTANCE AND FRAUDULENT AMOUNT RECOVERY SCHEME, 2026



CYBER CRIME VICTIM ASSISTANCE AND FRAUDULENT AMOUNT RECOVERY SCHEME, 2026

CHHATTISGARH STATE LEGAL SERVICES AUTHORITY

CYBER CRIME VICTIM ASSISTANCE AND FRAUDULENT AMOUNT RECOVERY SCHEME, 2026