UTTARAKHAND STATE LEGAL SERVICES AUTHORITY: CYBER SURAKSHA AND CYBER-FRAUD VICTIM ASSISTANCE SCHEME, 2026

UTTARAKHAND STATE LEGAL SERVICES AUTHORITY

High Court Campus, Nainital-263001, Telefax: 05942-236552, e-mail: slsa-uk@nic.in,
Website: https://uttarakhand.nalsa.gov.in
Portal For Free Legal Aid: https://nyaymitraslsa.uk.gov.in
Facebook Link: https://www.facebook.com/uttarakhand.slsa
Youtube Link: https://www.youtube.com/@ukslsa-uttarakhandstateleg6415
TOLL FREE No:- UKSLSA-18001804000, NALSA - 15100

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

S. No	Abbreviation	Full Form
1.	NALSA	National Legal Services Authority
2.	SLSA/UKSLSA	State Legal Services Authority/Uttarakhand State Legal Services Authority
3.	HCLSC	High Court Legal Services Committee
4.	DLSA	District Legal Services Authority
5.	PLV	Para-Legal Volunteer/AdhikarMitra
6.	SCHEME	Uttarakhand State Legal Services Authority: Cyber Suraksha and Cyber-Fraud Victim Assistance Scheme, 2026
7.	SCVSAC-Mitra	The State Cyber Victim Support and Awareness Cell
8.	DCLD	District Cyber Legal Aid Desks
9.	OTP	One-Time Password
10.	UPI	Unified Payments Interface
11.	ATM	Automated Teller Machine
12.	PIN	Personal Identification Number
13.	CVV	Card Verification Value
14.	FIR	First Information Report
15.	RBI	Reserve Bank of India
16.	NPCI	National Payments Corporation of India
17.	BNSS	Bharatiya Nagarik Suraksha Sanhita
18.	BNS	Bharatiya Nyaya Sanhita
19.	NCRP	National Cybercrime Reporting Portal
20.	CFCFRMS	Citizen Financial Cyber Fraud Reporting and Management System

UTTARAKHAND STATE LEGAL SERVICES AUTHORITY CYBER SURAKSHA AND CYBER-FRAUD VICTIM ASSISTANCE SCHEME, 2026

In exercise of the powers and functions conferred under Sections 2(c), 2(g), 7(2)(a), 7(2)(c), 7(2)(d), 8, 10 and 29A of the Legal Services Authorities Act, 1987, read with the National Legal Services Authority (Legal Services Clinics) Regulations, 2011 **and in compliance with the directions of the Supreme Court of India dated 04.08.2026 in S.M.W.P. (Crl.) No. 3 of 2025 titled *In re: Victims of Digital Arrest Related to Forged Documents****, the Uttarakhand State Legal Services Authority hereby formulates the Uttarakhand State Legal Services Authority: Cyber Suraksha and Cyber-Fraud Victim Assistance Scheme, 2026.

1. Short Title, Extent and Commencement

- **I.** This Scheme shall be called the ***"Uttarakhand State Legal Services Authority: Cyber Suraksha and Cyber-Fraud Victim Assistance Scheme, 2026."***
- **II.** It shall extend to the whole State of Uttarakhand.
- **III.** It shall come into force from the date of its approval by the Executive chairman of the Uttarakhand State Legal Services Authority *.
- **IV.** The Scheme shall be implemented through UKSLSA, District Legal Services Authorities, Tehsil Legal Services Committees, Legal Services Clinics, Front Offices, Para-Legal Volunteers and Panel Advocates.

2. Nature of the Scheme

- **I.** The awareness component shall be available to all persons residing in or visiting Uttarakhand.
- **II.** Free legal services shall be provided to persons fulfilling the eligibility requirements under Section 12 of the Legal Services Authorities Act, 1987 and UKSLSA Regulation.
- **III.** The Scheme shall provide legal awareness, emergency procedural assistance, coordination, legal advice, representation and assistance in accessing appropriate police, banking, judicial and victim-compensation remedies.

* Approved by the Hon'ble Executive Chairman, UKSLSA on 08.09.2026

IV. The Scheme shall not create an automatic right to reimbursement of the defrauded amount from UKSLSA funds.

V. Nothing in this Scheme shall confer investigative, banking, adjudicatory or fund-releasing powers upon UKSLSA or any DLSA.

VI. The actual freezing, holding, release or restoration of money shall remain subject to the action of the police, banks, payment-system operators, competent authorities and courts.

3. State Cyber Victim Support and Awareness Cell (SCVSAC-Mitra)

UKSLSA shall establish a **State Cyber Victim Support and Awareness Cell (SCVSAC-Mitra)** at the State level.The State Cell shall function under the administrative control of the Member Secretary, UKSLSA, subject to the overall supervision and directions of the Executive Chairman, UKSLSA.

The State Cell may consist of:-

I. A State Nodal Officer nominated by the Member Secretary.

II. One panel advocate experienced in cybercrime and financial fraud.

III. A representative of the Uttarakhand Police Cyber Crime Branch nominated by police Department.

IV. A technical or cyber-forensic resource person, if available.

V. A representative nominated by the State Bankers' Committee Uttarakhand.

VI. A victim-support or counselling representative nominated by the Member Secretary.

VII. Such other persons as may be nominated by the Member Secretary, UKSLSA.

Note-The inclusion of police, banking or technical representatives shall ordinarily be through nomination. They shall not be treated as employees of UKSLSA unless appointed in accordance with applicable law.

4. Functions of the State Cell

The State Cell shall:

I. Prepare and issue standard operating procedures, forms, awareness material and training modules.

II. Coordinate with NALSA, the Uttarakhand Police, Cyber Crime Branch, District Cyber Cells, banks, payment intermediaries, educational institutions and other stakeholders.

III. Coordinate with the Uttarakhand Cyber Crime Coordination Centre (S4C)(once notified),Uttarakhand nodal cyber office,Indian Cybercrime Coordination Centre (I4C) New Delhi and the State Bankers' Committee to operationalise the e-Zero FIR mechanism, MHA Grievance Redressal and Money Restoration Module.

IV. Maintain a State-level directory of police, bank, cybercrime, legal-aid and victim-support nodal officers.

V. Conduct training for DLSA staff, panel advocates and PLVs.

VI. Monitor the functioning of District Cyber Legal Aid Desks.

VII. Collect anonymised data and prepare monthly, quarterly and annual reports.

VIII. Develop bilingual public-awareness material in Hindi and English.

IX. Facilitate referral of cases involving vulnerable victims.

X. Review systemic problems relating to delayed reporting, bank complaints, account freezes, non-registration of complaints and restoration of held funds.

XI. Make recommendations to NALSA and the State Government for improvement of law, policy and institutional coordination.

XII. Coordinate with appropriate authorities regarding the implementation of the NCRP-CFCFRMS mechanism.

5. District Cyber Legal Aid Desks (DCLD)

Every DLSA shall establish a District Cyber Legal Aid Desk (DCLD) within its Front Office, Legal Services Clinic, District ADR Centre or at any other suitable premises, as deemed appropriate.The DCLD shall function under the direct administrative control and supervision of the concerned Secretary, DLSA, and shall discharge such functions and responsibilities as may be delegated or assigned to it by the UKSLSA from time to time.The Secretary, DLSA, shall be the ex-officio District Cyber Legal Aid Nodal Officer and shall oversee and coordinate the functioning of the DCLD. The Desk may consist of:-

I. District Cyber Legal Aid Nodal Officer (Secretary, DLSA).

II. One panel advocates as nominated by chairman, DLSA.

III. TwoTrained PLVsas nominated by chairman, DLSA.

IV. A police or cyber-cell liaison officer as nominated by SP/SSP Concerned.

V. A bank or financial-institution liaison contact, wherever formally nominated.

VI. A record-maintenance or data-entry officer.

Note-1:-The DLSA may establish additional cyber legal-aid clinics in villages, educational institutions, community centres, remote areas and other locations where access to legal services is difficult.

Note-2: The District Cyber Legal Aid Desks shall also function as specialised Legal Services Clinics under the National Legal Services Authority (Legal Services Clinics) Regulations, 2011.

6. Functions of District Cyber Legal Aid Desks (DCLD)

The District Cyber Legal Aid Desk shall:

I. Receive victims in person, by telephone or through referral.

II. Assist the victim in calling 1930 and reporting the fraud on the National Cybercrime Reporting Portal.

III. Assist the victim in contacting the bank, wallet provider, card issuer, payment app or other financial intermediary.

IV. Help the victim obtain complaint numbers, transaction references and acknowledgment receipts.

V. Assist in preparing a written complaint to the Cyber Crime Police Station or concerned police station.

VI. Help in preserving electronic and documentary evidence.

VII. Provide legal aid through Secretary, DLSA to eligible victims.

VIII. Assist in representations to the Superintendent of Police, District Cyber Officer, bank nodal officer or other competent authority.

IX. Facilitate applications relating to held, seized or traceable money.

X. Assist in appropriate applications before the competent court regarding custody, release, restoration, distribution or disposal of money.

XI. Maintain a confidential case register and submit periodic reports to UKSLSA.

XII. Assist victims in filing grievances under the MHA Grievance Redressal and Money Restoration Module and the RBI Integrated Ombudsman Scheme, where applicable.

XIII. Facilitate registration of e-Zero FIR and NCRP complaints in coordination with the District Cyber Cell.

7. Relationship with Existing Authorities

The State Cyber Victim Support and Awareness Cell (SCVSAC-Mitra) and District Cyber Legal Aid Desks (DCLD) shall function as legal-services and victim-assistance mechanisms. They shall not:

I. Register or investigate offences.

II. Direct the police to freeze or release an account.

III. Direct a bank to reverse a transaction.

IV. Decide ownership of disputed money.

V. Conduct forensic examination.

VI. Guarantee recovery.

VII. Collect money, passwords, PINs, OTPs or remote access from victims.

VIII. Engage private recovery agents on behalf of UKSLSA.

Note:-The State Cell may seek coordination and status updates from the police, banks and other institutions, but the statutory powers of those institutions shall remain unaffected.

8. Public-Awareness Programme

DLSAs shall conduct a continuing public-awareness campaign once in every quarter under the theme:

STOP – THINK – VERIFY – REPORT

The campaign shall include:

I. Legal-awareness camps in Schools, Colleges, Universities, Rural and Urban Areas.

II. Senior-citizen awareness programmes.

III. Training for women's groups, Mahila Mangal Dal, traders, migrant workers and government employees.

IV. Camps at banks, post offices, Common Service Centres and public offices.

V. Mobile legal-awareness vans in remote and hilly areas.

VI. Radio, newspapers, television and social-media campaigns.

VII. Posters, pamphlets, short videos and street plays.

VIII. Legal-literacy clubs and community-level programmes through PLVs.

9. Minimum Awareness Messages

Every awareness material shall, as far as possible, include the following:

I. There is no legal concept of *"digital arrest."*

II. Genuine police officers, courts and government agencies do not arrest persons through video calls.

III. No genuine authority demands money for avoiding arrest or closing a criminal case.

IV. Do not share OTP, UPI PIN, ATM PIN, CVV, passwords or screen access.

V. Do not install an application at the request of an unknown caller.

VI. Do not click unknown links or scan an unknown QR code for receiving money.

VII. Independently verify any call claiming to be from the police, CBI, ED, RBI, TRAI, bank, courier or telecom department.

VIII. Do not transfer money merely because a caller threatens arrest, account closure or seizure of property.

IX. Report financial cyber fraud immediately by calling 1930 and through www.cybercrime.gov.in.

X. Inform the bank or payment provider immediately.

XI. Preserve all call records, chats, emails, screenshots, payment details and documents.

XII. The Supreme Court of India has directed immediate reporting through 1930 and the National Cybercrime Reporting Portal and advises citizens to verify the identity of callers and consult trusted persons before transferring money.

XIII. Information on the MHA Grievance Redressal and Money Restoration Module shall be disseminated in all awareness material.

10. Eligibility and Priority Groups

The awareness component shall be available to every member of the public. Legal services shall be provided to persons satisfying Section 12 of the Legal Services Authorities Act, and UKSLSA, Regulation, including women, children, members of Scheduled Castes or Scheduled Tribes, persons with disabilities, persons in custody, industrial workmen, persons in circumstances of undeserved want and persons satisfying the applicable income criterion. Priority shall be given to:

- **I.** Senior citizens.
- **II.** Women and children.
- **III.** Persons with disabilities.
- **IV.** Persons from Scheduled Castes and Scheduled Tribes.
- **V.** Persons living in remote, hilly or difficult-to-access areas.
- **VI.** Persons with limited digital literacy.
- **VII.** Persons who have lost pension, medical, educational or life-savings funds.
- **VIII.** Persons subjected to intimidation, blackmail or prolonged video-call confinement.
- **IX.** Victims whose accounts have been frozen due to a cybercrime investigation.
- **X.** Persons requiring immediate rehabilitation or counselling.

11. Immediate-Response Protocol

When a victim approaches a DLSA, Legal Services Clinic, PLV or Front Office, the following procedure shall be followed.

A. Stop further loss:-The victim shall be advised to:

- **I.** Disconnect from the fraudster.
- **II.** Stop all further payments.
- **III.** Block compromised cards or payment instruments.
- **IV.** Contact the bank through its official channel.
- **V.** Change passwords from a secure device.
- **VI.** Remove remote-access applications.
- **VII.** Avoid negotiating with or threatening the fraudster.
- **VIII.** Avoid paying any person who promises guaranteed recovery.

B. Report immediately:-The victim shall be assisted to:

- **I.** Call 1930.
- **II.** File a complaint on the National Cybercrime Reporting Portal (NCRP).
- **III.** Inform the bank, card issuer, wallet provider, payment app or other financial intermediary.

IV. Request a transaction dispute, reversal, chargeback, lien or hold, wherever factually and legally applicable.

V. Obtain complaint numbers, ticket numbers and transaction reference numbers.

VI. Submit or follow up on a written complaint before the Cyber Crime Police Station or concerned police station.

Note:-The NCRP-CFCFRMS mechanism is intended to facilitate prompt reporting, tracing of the money trail and placing the reported amount on hold. The National SOP {the National Cybercrime Reporting Portal (NCRP) and the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS)} also provides processes relating to custody, restoration, court orders and grievance redressal.

C. Preserve evidence:-The victim shall be assisted in preparing an evidence file containing:

I. NCRP acknowledgement.

II. 1930 complaint or ticket number.

III. FIR or e-FIR, if registered.

IV. Bank complaint and dispute number.

V. Bank statement.

VI. UTR, RRN, IMPS, NEFT, RTGS or UPI reference number.

VII. Fraudster's account number, UPI ID, wallet or merchant details.

VIII. Mobile numbers and email IDs.

IX. Screenshots of chats, websites, advertisements and payment requests.

X. Call details and recordings, where lawfully available.

XI. Details of remote-access applications.

XII. Fake notices, warrants, identity cards or departmental documents.

XIII. Identity and bank-account documents of the victim.

XIV. A chronological statement of events.

Note:-The original device and electronic evidence shall be preserved safely. Screenshots or recordings should not be edited or manipulated.

12. Recovery Assistance Track

Each DLSA in the state shall operate a Cyber-Fraud Recovery Assistance Track consisting of the following stages:

Stage	Action
Stage I: Emergency reporting	1930 call, NCRP complaint and immediate bank notification.
Stage II: Evidence preparation	Preparation of a chronological statement and transaction chart.
Stage III: Money-trail follow-up	Coordination with the investigating officer regarding beneficiary accounts and intermediary accounts.
Stage IV: Hold-status follow-up	Follow-up regarding the amount placed on hold through the competent police and banking channels.
Stage V: Legal application	Preparation of an appropriate application for custody, release, restoration or distribution of the held amount.
Stage VI: Multiple-victim cases	Assistance in seeking identification of genuine victims and equitable or pro-rata distribution where funds are commingled.
Stage VII: Non-recovery cases	Advice regarding investigation, compensation, banking grievances, consumer remedies and other lawful options.

13. Legal Remedies for Restoration

The panel advocate may, depending on the facts:

- **I.** Request the Investigating Officer to trace the amount and place it on hold at every identifiable level.
- **II.** Assist in proceedings relating to custody, release, disposal or restoration of money under the applicable provisions of the Bharatiya Nagarik Suraksha Sanhita, 2023.

III. Consider applications under Sections 107, 497, 498 and 503 of the BNSS, wherever applicable.

IV. Assist in applications for equitable or pro-rata distribution in multiple-victim cases.

V. Assist the victim in seeking compensation under Section 395 of the BNSS at the stage of conviction, where appropriate.

VI. Assist in an application under Section 396 of the BNSS where the victim requires rehabilitation and the requirements of the applicable State victim-compensation scheme are satisfied.

VII. Assist in approaching the appropriate banking grievance mechanism or RBI Integrated Ombudsman Scheme, where the facts disclose an unauthorised electronic transaction or deficiency in banking service.

VIII. Assist the victim in filing a grievance under the MHA Grievance Redressal and Money Restoration Module and the RBI Integrated Ombudsman Scheme, where the facts disclose an unauthorised electronic transaction or deficiency in banking service.

Note-The current national SOP{the National Cybercrime Reporting Portal (NCRP) and the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS)}specifically recognises court and police processes concerning money held or seized in cyber-fraud cases, including proceedings under Sections 497, 498 and 503 of the BNSS.

14. Banking-Liability Caution

The Panel Advocate shall explain that:

I. Prompt reporting improves the possibility of stopping or tracing the money.

II. Recovery is not automatic.

III. RBI rules concerning unauthorised electronic transactions require early reporting to the bank.

IV. Where a victim personally authorised a payment after being deceived, the question of bank liability must be examined on the facts.

V. Sharing credentials, negligence, authentication, consent, system failure and the conduct of the bank may all be relevant.

VI. A held amount is not the same as a recovered amount.

Note:-RBI materials advise customers to inform the bank immediately about unauthorised electronic transactions and recognise that the time taken to report may affect customer liability.

15. Victim-Compensation Interface

I. This Scheme shall not be interpreted as creating anentitlement to reimbursement of the stolen amount from UKSLSA funds.

II. The DLSA shall assist an eligible victim in applying under the applicable Uttarakhand Victim Compensation Scheme in appropriate cases.

III. Where the facts do not fall within the existing victim-compensation framework, UKSLSA may submit a recommendation to the State Government for expansion of victim compensation categories to include digital arrest and cyber-fraud victims, pending the national framework directed by the Supreme Court.

IV. Compensation and recovery of crime proceeds shall be recorded separately.

16. Roles of Stakeholders

A. UKSLSA

UKSLSA shall:

I. Approve the Scheme and operational guidelines.

II. Establish the State Cell.

III. Nominate State nodal officer.

IV. Conduct trainings.

V. Coordinate with police, banks and other agencies.

VI. Monitor implementation.

VII. Prepare quarterly and annual reports.

B. DLSAs

DLSAs shall:

I. Establish District Cyber Legal Aid Desks (DCLD).

II. Receive and register victim requests.

III. Provide or arrange legal aid.

IV. Conduct awareness programmes and trainings.

V. Monitor recovery-assistance cases.

VI. Refer appropriate cases for compensation and rehabilitation.

VII. Submit monthly reports to UKSLSA.

C. PARA-LEGAL VOLUNTEERS

PLVs shall:

I. Identify vulnerable victims.

II. Conduct community awareness.

III. Assist victims in reaching 1930, NCRP and the bank.

IV. Help collect basic facts and documents.

V. Maintain confidentiality.

VI. Never seek OTPs, PINs, passwords or money.

VII. Never promise recovery.

VIII. Refer legal questions to the DLSA or panel advocate.

D. PANEL ADVOCATES

Panel advocates,on the assignment of matter, shall:

I. Provide competent and victim-sensitive legal assistance.

II. Explain the realistic prospects and limitations of recovery.

III. Assist in complaints, representations and court applications.

IV. Avoid guarantees of recovery.

V. Maintain confidentiality.

VI. Disclose conflicts of interest.

VII. Not charge fees from legally aided victims for assigned services.

17. Service Standards

Subject to police, banking and judicial processes, the following timeline may be followed:

I. Assistance in contacting 1930 and the bank: **immediately**.

II. Acknowledgment of a request by the DLSA: **immediately or within one working day**.

III. Assignment of a panel advocate in an eligible case: **within two working days**.

IV. Preparation of a recovery action plan: **within seven working days after receipt of essential documents**.

V. Review of pending cases: **every fifteen days**.

VI. Monthly reporting by DLSAs.

VII. Quarterly review by the State Cell.

Note- These are administrative targets and do not constitute a guarantee of freezing, recovery, investigation or judicial disposal.

18. Confidentiality and Data Security

I. Information shall be collected only for providing legal assistance, making referrals, pursuing remedies and preparing anonymised reports.

II. No UKSLSA or DLSA officer, PLV or advocate shall ask for an OTP, UPI PIN, ATM PIN, password or remote access.

III. Victim names, photographs, phone numbers and financial details shall not be published without lawful authority and informed consent.

IV. Access to the case register shall be restricted to authorised personnel.

V. Sensitive electronic records shall be stored securely and transmitted only through authorised channels.

VI. Data shall not be shared with private recovery agents, unauthorised persons or media organisations.

19. Monitoring Indicators

The State Cell and DLSAs shall maintain the following data:

I. Number of awareness programmes.

II. Number of persons reached.

III. Number of trained PLVs and advocates.

IV. Number of victims assisted.

V. Number of 1930 and NCRP referrals.

VI. Number of bank complaints facilitated.

VII. Number of FIRs or e-FIRs registered.

VIII. Amount placed on hold, restored or released and recovery applications filed.

IX. Number of compensation applications filed.

X. Number of matters involving senior citizens, women, children and persons with disabilities.

XI. Average time between fraud and reporting.

XII. Number of complaints concerning wrongful freezing of accounts.

XIII. Number of grievances filed under the MHA Grievance Redressal and Money Restoration Module.

XIV. Number of grievances filed under the RBI Integrated Ombudsman Scheme.

XV. Amount restored through the MHA money restoration module.

Note- The amount reported, the amount placed on hold and the amount restored shall be recorded separately.

20. Review and Amendment

The Scheme shall be reviewed annually or earlier if required due to:

I. Amendments to the BNSS, BNS, Information Technology Act or banking regulations.

II. Directions of the Supreme Court or High Court.

III. Directions or schemes issued by NALSA, MHA, I4C, RBI, NPCI or other competent authorities.

IV. Changes in the NCRP-CFCFRMS mechanism.

V. Experience of victims and DLSAs.

VI. Emergence of new cyber-fraud methods.