LEGAL SERVICES OF LONG ISLAND

P.O. Box 1907
Suwanee, GA 30024

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>
Enrollment Deadline: September 1, 2026

To Enroll, Scan the QR Code Below:

Scan Me

Or Visit:
https://response.idx.us/legalservicesli

June 1, 2026

Notice of Security Incident

Dear <<First Name>> <<Last Name>>:

We are writing to inform you of a data incident (the "Incident") at Legal Services of Long Island, Inc. ("LSLI" or "we") that may have impacted your personal information. LSLI is a legal services organization that assists low-income individuals in resolving housing issues and obtaining governmental benefits and provides various outreach and community education programs. As part of the services it provides, LSLI received certain personal information of yours. Although we are unaware of any actual identity theft or fraud directly related to the Incident, out of an abundance of caution we are providing you with information about the Incident, our response, and the steps we are offering on your behalf. We take the protection of your personal information very seriously and want to provide you with details, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On or around November 23, 2025, LSLI discovered suspicious activity within our technical environment and immediately engaged cybersecurity and data forensic specialists to contain the incident, terminate unauthorized access, and assess any potential impact to the LSLI computing environment. On January 5, 2026, the data forensic specialists recovered and began reviewing files accessed by an unauthorized third party. On May 15, 2026, the investigation determined that an unauthorized third party accessed certain systems and removed data that may be connected to this Incident.

What Information was Involved?

The following data elements may have been involved: address, date of birth, Social Security number, <<Variable Data 1>> and personal health information such as diagnosis information, treatment information, and doctor/medical professional name. To date, we have found no evidence to indicate that your personal information was misused in any way.

What We Are Doing.

In addition to engaging cybersecurity counsel and digital forensics specialists to conduct a thorough investigation, we took immediate action to prevent further access. We reset all account passwords related to the breach, severed the unauthorized user's access to our system, and took further steps to prevent further access. Additionally, we are implementing enhanced technical and administrative security measures across our network to help prevent further security incidents. We reiterate that we contained the damage and have no evidence of misuse.

Additionally, we are offering identity theft protection services, through IDX, a data breach and recovery services expert. IDX identity theft protection services include: <<12/ 24>> months of 24/7 credit monitoring, a $1,000,000 insurance reimbursement policy, and CyberScan, a tool that searches the dark web to see if your information has been potentially exposed to cyber criminals. With these protections, IDX will help you resolve issues if your identity is compromised. IDX identity theft protection services are offered at no charge. We encourage you to take full advantage of this service offering.

What You Can Do.

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-855-759-9333, going to https://response.idx.us/legalservicesli, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information.

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-855-759-9333 or go to https://response.idx.us/legalservicesli for assistance or for any additional questions you may have.

Sincerely,

Legal Services of Long Island, Inc.

Recommended Steps to Help Protect Your Information

1. Website and Enrollment. Scan the QR image or go to https://response.idx.us/legalservicesli and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is September 1, 2026.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-855-759-9333 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General. You have the right to obtain a police report.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** https://oag.maryland.gov, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.