



Secure Processing Center
P.O. Box 680
Central Islip, NY 11722-0680

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

June 15, 2026

Dear <<Full Name>>,

We are writing to inform you that Lance Soll & Lunghard, LLC (“LSL” or “we”) experienced a data incident (the “Incident”) that potentially involved your personal information (“Information”). This letter provides you with information about this Incident, our response, steps you can take, and information on where to direct your questions. Additionally, as a precaution we have also provided steps you can take to protect your Information, including the ability to enroll in credit monitoring services that we are offering free of charge for <<CM Duration>>.

What Happened?

On April 27, 2026, LSL detected unusual activity within our tax preparation software and discovered that a limited number of potentially fraudulent tax returns had been filed using information of a limited number of our clients. We immediately began an investigation and took steps to remediate any activity within our computer systems that could be related to the Incident. This included changing passwords, obtaining a new EFIN, and engaging cybersecurity and privacy professionals to assist in our response.

Our investigation identified that an unauthorized actor gained access to one (1) employee’s workstation from March 19, 2026, to April 27, 2026, when we discovered and contained the Incident. The unauthorized actor accessed your Information in an attempt to improperly collect funds from the federal government and state tax authorities. We have reported this matter to the appropriate regulatory authorities, including the Internal Revenue Service (“IRS”) and law enforcement. Besides this effort to defraud the government, the investigation did not identify other misuse of information related to the Incident.

What Information Was Involved?

We determined that the following types of Information may have been impacted as a result of this Incident: name and Social Security Number.

What We Are Doing.

We take this Incident and the security of information in our care very seriously. Upon becoming aware of the Incident, we notified the IRS and have since worked closely with state tax authorities to share information and take steps to protect our clients’ information. We are also exploring what additional measures we can implement to enhance our already robust security protections. After determining unauthorized activity occurred on our systems, we immediately began analyzing the information involved and engaged data security and privacy professionals to aid in our response and notify affected individuals and relevant government agencies of this Incident.

What Can You Do?

To help protect your identity and address any concerns, we are offering complimentary access to credit monitoring services through Epiq – Privacy Solutions ID, for <<CM Duration>> months. To start monitoring your personal information, please follow the steps below:

1. Visit www.privacysolutionsid.com and click “Activate Account.”
2. Enter the following activation code, <<Activation Code>> and complete the enrollment form.
3. Complete the identity verification process.
4. You will receive a separate email from noreply@privacysolutions.com confirming your account has been set up successfully and will include an Access Your Account link in the body of the email that will direct you to the log-in page.
5. Enter your log-in credentials.
6. You will be directed to your dashboard and activation is complete.

The deadline to enroll is <<Enrollment Deadline>>. If you need assistance with the enrollment process or have questions regarding Epiq – Privacy Solutions ID, please call the toll-free assistant line at (866) 675-2006, Monday through Friday 8:00am to 4:30pm Central Time.

Additionally, it is always recommended that you remain vigilant, regularly monitor free credit reports, review account statements, and report any suspicious activity to financial institutions. Please also review the “Additional Resources” section included with this letter, which outlines other resources you can utilize to protect your Information.

For More Information.

We take this Incident and the security of information in our care seriously. If you have additional questions, please reach out to your Partner. You may call us at 949-829-8299 Monday through Friday 8 am – 5 pm PST (excluding U.S. holidays).

Sincerely,



Bryan Gruber, CPA
Managing Partner

Encl.

ADDITIONAL RESOURCES

Contact information for the three (3) nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com/personal/credit-report-services, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com/help, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, <https://www.transunion.com/data-breach-help>, 1-833-395-6938

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every twelve (12) months from each of the three (3) nationwide credit reporting agencies.

To order your annual free credit report please visit www.annualcreditreport.com or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Massachusetts, and New Jersey residents: You may obtain one (1) or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one (1) of the three (3) nationwide credit reporting agencies above. 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.

Security Freeze. You may obtain a security freeze on your credit report, free of charge, to protect your privacy and confirm that credit is not granted in your name without your knowledge. You may also submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report, free of charge, or submit a declaration of removal pursuant to the Fair Credit Reporting Act ("FCRA").

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three (3) credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for them as well): (1) full name, with middle initial, and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or Department of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

FTC and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the FTC and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

Reporting of identity theft and obtaining a police report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Arizona Residents: You can obtain information from the Office of the Attorney General and the FTC about fraud alerts, security freezes, and steps you can take toward preventing identity theft. Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004, 1-602-542-5025.

For 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, 1-800-952-5225. This notification was not delayed as a result of any law enforcement investigation.

For Colorado Residents: You can obtain information from the Office of the Attorney General (www.coag.gov), FTC, and the credit reporting agencies about fraud alerts and security freezes. Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203, 1-720-508-6000.

For Connecticut Residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, www.ct.gov/ag, 1-860-808-5318.

For Illinois Residents: You can obtain information from the Office of the Attorney General, credit reporting agencies, and the FTC about fraud alerts and security freezes (contact information above). You may contact the Illinois Office of the Attorney General, 100 West Randolph Street, Chicago, IL 60601, https://illinoisattorneygeneral.gov/about/email_ag.jsp, 1-800-964-3013.

For Massachusetts Residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html. You have the right to obtain a police report if you are a victim of identity theft.

For Minnesota Residents: You may contact the Minnesota Office of the Attorney General, 445 Minnesota Street, Suite 1400, St. Paul, MN 55101, www.ag.state.mn.us, 1-800-657-3787.

For Nevada Residents: You may contact the Nevada Office of the Attorney General, Bureau of Consumer Protection, 100 N. Carson St, Carson City, NV 89701, www.ag.nv.gov, 1-702-486-3132.

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

For New York Residents: You may obtain information regarding security breach response and identity theft prevention and protection information from the FTC (contact information above) and the New York Office of the Attorney General, Office of the Attorney General, The Capitol, Albany, NY 12224-0341, <https://ag.ny.gov>, 1-800-771-7755.

For North Carolina Residents: You may obtain information about preventing identity theft from the FTC (contact information above) and the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Main Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7266 or 1-919-716-6400. You are advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Pennsylvania Residents: You may contact the Pennsylvania Office of the Attorney General, Bureau of Consumer Protection, 15th Floor, Strawberry Square, Harrisburg, PA 17120, www.attorneygeneral.gov, 1-800-441-2555.

For Texas Residents: You may contact the Texas Office of the Attorney General, Office of the Attorney General, PO Box 12548, Austin, TX 78711-2548, www.texasattorneygeneral.gov, 1-800-621-0508.

For Wyoming Residents: This notification was not delayed as a result of any law enforcement investigation.

How to Apply for an IRS Identity Protection PIN

- Go to: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.
- Select the button: "Get an IP PIN."
- The fastest way to receive an IP PIN is to request one through your ID.me account, under your "Profile" page. If you don't already have an account on IRS.gov, you must register to validate your identity.
- Spouses and dependents are eligible for an IP PIN if they can pass the identity verification process.
- Once you have opted in and obtained an IP PIN online, you will need to retrieve your IP PIN online each calendar year as a CP01A Notice will not be mailed. The IP PIN is generally available in your online account starting in mid-January through mid-November.

If you need help applying for this PIN, please call our office.

The IRS offers a sign-in option with ID.me, which offers access to IRS online services with a secure account that protects your privacy.
ID.me is an account created, maintained, and secured by a technology provider.
If you don't have an ID.me account, you must create a new account.

Sign in with an existing account

Sign in with **ID.me**

OR

Create a new account

ID.me Create an account