

Return to Kroll
P.O. Box 3826
Suwanee, GA 30024

Hamill & Kaplan, LLP
340 N. Westlake Blvd, Suite 220
Westlake Village, CA 91362



August 3, 2026

NOTICE OF DATA BREACH

Dear [REDACTED]

Please read this letter in its entirety.

We are writing to provide you with a formal notification regarding a data incident that occurred at the office of Hamill & Kaplan, LLP, in which your sensitive information may have been accessible to an unauthorized user. This letter serves to provide additional information concerning the incident, what is being done to correct it, and what you can do to further protect your information.

What Happened?

On September 19, 2025, we discovered that an unauthorized user gained access to our computer network earlier that day. The threat actor was able to access some of our company's files which included your personal information. While we have no information that your sensitive data has been misused by the unauthorized user, we are providing you with notice so that you may be proactive in protecting your data.

Following our discovery of the breach, we immediately took measures to ensure our network was secure and began an investigation with the assistance of third-party IT specialists to determine the full nature and scope of this incident. The investigation has recently concluded, and at this time, the investigation has shown that your sensitive personal information may have been accessible to the threat actor during the breach. Unfortunately, these types of incidents are becoming increasingly common and organizations with some of the most sophisticated IT infrastructure available continue to be affected.

We are taking appropriate precautionary measures to protect your financial security and to help alleviate concerns you may have. If we become aware of any suspicious activity in connection with your tax returns, we will notify you immediately. Conversely, if you receive any notifications from the IRS concerning suspicious activity on your account, please notify us or your current tax preparer right away.

What Information Was Involved?

Our investigation has revealed that some sensitive information may have been accessed, such as your social security number, other government identification numbers, name, bank account information, and/or other sensitive information you may have also provided to us.

What We Are Doing.

As soon as we discovered the incident, we took the steps described above. We also hired a third party to perform a thorough review of our systems to investigate the incident and enhance our network security. We continue our work with outside cybersecurity experts to reinforce our systems and security protocols in an effort to prevent incidents from occurring in the future.

We have also notified the FBI, IRS, Franchise Tax Board, and Secret Service of this incident. This notification to you was not delayed as a result of law enforcement investigation.

If we learn that your sensitive information has been compromised beyond what is described in this letter, we will let you know immediately.



We are taking this matter very seriously and are committed to helping those people who may have been impacted by this unfortunate situation.

What You Can Do.

Please review the “*Steps You Can Take to Help Protect Your Information*” on the next page to understand how you can protect your sensitive information and see the instructions for signing up for Credit Monitoring Services.

For More Information.

Should you have additional questions or concerns regarding this matter, please do not hesitate to contact (844) 958-8935, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

Hamill & Kaplan, LLP

Steps You Can Take to Help Protect Your Information

What You Can Do.

Please do the following:

You can obtain Credit Monitoring by contacting one of the three major credit agencies directly at:

Experian (1-888-397-3742)
P.O. Box 4500
Allen, TX 75013
www.experian.com

Equifax (1-800-525-6285)
P.O. Box 740241
Atlanta, GA 30374
www.equifax.com

TransUnion (1-800-680-7289)
P.O. Box 2000
Chester, PA 19016
www.transunion.com

- Obtain free copies of your credit report and monitor them upon receipt for any suspicious activity.
- Contact any of these three major credit bureaus to place a free fraud alert on your credit file. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on the credit report for one year, after which you can renew if desired.
- If you haven't already, we strongly suggest you contact the IRS about getting an Identity Protection PIN to use with your Social Security Number for heightened security. You can do this by going to <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.
- Remember, the IRS will never call you on the phone to demand information, money, or threaten you with arrest. Any IRS correspondence would be received in the form of a Notice or Letter. Please let us know if you receive any IRS correspondence regarding this incident so we can assist you with the response.
- Further, we recommend you change any passwords, usernames, or security questions that you may have shared with us.
- We strongly recommend you be vigilant in reviewing your bank accounts and other financial account statements, as well as monitoring your Credit Monitoring or free credit reports.
- If you suspect fraudulent activity, report it to law enforcement, including the Federal Trade Commission at <https://www.identitytheft.gov/#/> and your State Attorney General's Office at <https://www.naag.org/find-my-ag/>.
- You can obtain more information from the Federal Trade Commission and your State Attorney General's Office about identity theft, fraud alerts, security freezes, and the protection of your sensitive information. The Federal Trade Commission can be contacted as follows:
 - **Federal Trade Commission**
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-382-4357
<https://www.consumer.ftc.gov/>