

Perkins Law Provides Notice of Data Security Incident

The privacy and security of protected health information is of the utmost importance to Perkins Law. This notice contains information regarding a data security incident that involved certain protected personal information collected and maintained by Perkins Law. Perkins Law is providing individuals with information about the incident and the services being made available to those who are involved. Perkins Law continues to take significant measures to protect personal information.

Perkins Law experienced a security incident that impacted their network on or about October 9, 2024. Upon learning of this issue, Perkins Law immediately contained and secured the threat and commenced a prompt and thorough investigation. As part of the investigation, Perkins Law engaged external cybersecurity professionals experienced in handling these types of incidents to determine the extent of any compromise of the information on the Perkins Law network. Based on the comprehensive investigation, Perkins Law concluded that certain documents and records maintained within their possession were accessed and/or obtained in connection with this incident. Following the extensive manual document review, Perkins Law determined on January 7, 2025 that certain personal information was present in those documents and records. The impacted data includes full name in combination with Social Security number, date of birth, account number and routing number. Not all data elements were impacted for every resident.

To date, Perkins Law is not aware of any incidents of identity fraud or financial fraud as a result of the incident. Nevertheless, out of an abundance of caution, Perkins Law is providing notice to the affected clients commencing on January 22, 2025 in substantially the same form as the enclosed letter (Attached as Exhibit A). The notified individuals who have had their Social Security number impacted will receive complimentary credit monitoring services. Additionally, Perkins Law will advise all affected residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Perkins Law will further advise the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Individuals who have questions or need additional information regarding this incident or to determine if they are notified may reach out to the toll-free response line that Perkins Law has set up to respond to questions at 1-800-405-610. This response line is available Monday through Friday 8:00 a.m. to 8:00 p.m. Eastern Time (excluding major U.S. holidays).

* * *

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

You may place an initial one-year “Fraud Alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348-5069

Experian
P.O. Box 9554
Allen, TX 75013

TransUnion
Fraud Victim Assistance
Department

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

<https://www.experian.com/fraud/center.html>
(888) 397-3742

P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

2. **Placing a Security Freeze on Your Credit File.**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “security freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance
Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

3. **Obtaining a Free Credit Report.**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. **Additional Helpful Resources.**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the

police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.