

Schlesinger Law Offices, P.A. Notifies Affected Individuals of Information Security Incident

The privacy and security of the personal and confidential client information we maintain is of the utmost importance to Schlesinger Law Offices, P.A.

What Happened?

We discovered unauthorized access to our network occurred between March 20, 2024, and March 26, 2024.

What We Are Doing.

We immediately launched an investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations to analyze the extent of any compromise of the information on our network.

What Information Was Involved?

Based on our comprehensive investigation and document review, which concluded on November 20, 2025, we discovered that a limited amount of personal information may have been removed from our network in connection with this incident, including full names and one or more of the following: Social Security numbers, dates of birth, driver's license numbers or state identification numbers, other government identification numbers, financial account information, credit or debit card information, usernames and passwords, health insurance policy information, and/or medical information. Other confidential information may have also been impacted.

What You Can Do.

To date, we are not aware of any reports of identity fraud or improper use of any information as a direct result of this incident. Out of an abundance of caution, we are providing this notification. Below are steps affected individuals may take in order to protect themselves, including enrolling in complimentary credit monitoring services (if Social Security number was impacted), placing a fraud alert/security freeze on their credit files, obtaining free credit reports, remaining vigilant in reviewing financial account statements and credit reports for fraudulent or irregular activity, and taking steps to safeguard against medical identity theft.

For More Information.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal and confidential information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of personal and confidential information.

Individuals with questions concerning this incident or who would like to inquire whether they were impacted may call a dedicated and confidential toll-free response line that we have set up to respond to questions at 855-720-3748. The response line is available Monday through Friday, 9:00am to 9:00pm, Eastern Time.

– OTHER IMPORTANT INFORMATION –

Enrolling in Complimentary Credit Monitoring.

Affected individuals whose Social Security numbers were impacted are eligible to enroll in complimentary credit monitoring services. Individuals who would like to inquire whether they were impacted and are eligible for complimentary credit monitoring services may call a dedicated and confidential toll-free response line that we have set up to respond to questions at **855-720-3748**.

Placing a Fraud Alert on Your Credit File.

We recommend that you 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
<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

Consider 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 Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
(888)-298-0045

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://experian.com/freeze>
(888) 397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
<https://www.transunion.com/credit-freeze>
(888) 909-8872

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 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.

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.

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.

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.

Protecting Your Medical Information.

As a general matter, the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

###