Notice of Cybersecurity Event

Updated February 5, 2026

Apex Spine and Neurosurgery, LLC publishes this notice of a computer network security event. This notice provides individuals with information about what happened, steps we have taken in response, and steps individuals may take should they feel it is appropriate.

What Happened? On December 23, 2025, we learned that an unknown cyber actor accessed a portion of our computer network and installed a computer virus to lock files on computer systems. In response, we securely recovered the computer network and investigated what occurred. During this investigation, we learned that the cyber actor copied files from the computer network on December 9. The files are being reviewed to determine what information was contained in them, and to whom the information relates. This file review is ongoing. However, in the interest of disclosing this matter as soon as possible, we are publishing this notice on our website and providing free resources and guidance as detailed further below. After the file review is complete, we will mail letters to individuals for whom we have available address information.

What Information Was Involved? The types of information present in the copied files varies by individual but can collectively contain name and the following: demographic identifiers, which could include address, phone number, date of birth, Social Security number, driver's license number, passport number, other government identifier(s); health information, which could include location of health services, dates of service, treatment or condition information, diagnosis, diagnosis code, prescription information, history information, assigned physician; health services payment information, such as financial account number without a security code, access code, or password to access an account, health insurance information subscriber or identification number, and patient account number.

What Information Is Not Involved? Our Electronic Health Records platform is maintained in a logically separated computer network environment and was not impacted by this event.

What We Are Doing. We are notifying individuals to ensure they are aware of this matter. Direct notices will be mailed to individuals for whom we have contact information at the conclusion of the data review, which is necessary to determine whose information may be involved with this event. Additionally, we are providing individuals guidance on how to protect their information, should they feel the need to do so. While no safeguards can fully prevent all cybersecurity matters, we are evaluating additional technical measures, as well as reviewing our cyber auditing practices, to reduce the risk of an issue like this reoccurring. We will continue to evaluate and update our policies and practices as appropriate.

What You Can Do. We encourage individuals to remain vigilant against incidents of identity theft and fraud by reviewing their account statements, including explanation of benefits, and monitoring their free credit reports for suspicious activity and to detect errors. We also encourage individuals to review the below "Steps Individuals Can Take To Protect Personal Information" section. This section contains free resources that are available, including guidance for monitoring free credit reports, how to place a fraud alert or security freeze on credit files, and contact information for the consumer reporting agencies and Federal Trade Commission.

For More Information. If individuals have questions about this matter, they may write to us at Apex Spine and Neurosurgery, Attn: Compliance, 454 Satellite Boulevard, Suite 101, Suwanee, GA 30024. At the conclusion of the data review, we will send direct notices to individuals for whom contact information is available and will have call center representatives available to help answer questions.

Sincerely,

Apex Spine and Neurosurgery

STEPS INDIVIDUALS CAN TAKE TO PROTECT PERSONAL INFORMATION

Monitor Relevant Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax—www.equifax.com; 1-888-298-0045; and P.O. Box 105788 Atlanta, GA 30348-5788
Experian—www.experian.com; 1-888-397-3742; and P.O. Box 9554, Allen, TX 75013
TransUnion—www.transunion.com; 1-833-799-5355; and P.O. Box 160, Woodlyn, PA 19094

For loved ones that may have recently passed, individuals may also place a "deceased – do not issue credit" flag on the loved one's credit file. Only one consumer reporting bureau needs to be notified, and it will notify the other two major consumer reporting bureaus. Individuals may complete this process using the information provided by the credit bureaus at the below websites:

Equifax: https://www.equifax.com/personal/help/article-list/-/h/a/relative-death-contact-credit-bureaus
Experian: https://www.experian.com/blogs/ask-experian/reporting-death-of-relative/
TransUnion: https://www.transunion.com/blog/credit-advice/reporting-a-death-to-tu

STEPS INDIVIDUALS CAN TAKE TO PROTECT THEIR MINOR DEPENDENTS' PERSONAL INFORMATION

Monitor Relevant Accounts

Typically, credit reporting agencies do not have a credit report in a minor's name. To find out if your minor dependent has a credit report or to request a manual search for your minor dependent's Social Security number, each credit bureau has its

own process. To learn more about these processes or request these services, you may contact the credit bureaus by phone or in writing or you may visit or contact the below credit bureaus.

Equifax—www.equifax.com; 1-888-298-0045; and P.O. Box 105788 Atlanta, GA 30348-5788
Experian—www.experian.com; 1-888-397-3742; and P.O. Box 9554, Allen, TX 75013
TransUnion—www.transunion.com; 1-833-799-5355; and P.O. Box 160, Woodlyn, PA 19094

To request information about the existence of a credit file in your minor dependent's name, search for your dependent's Social Security number, place a security freeze on your dependent's credit file, place a fraud alert on your dependent's credit report (if one exists), or request a copy of your dependent's credit report you may be required to provide some or all the following information:

- A copy of your driver's license or another government issued identification card, such as a state identification card, etc.;
- Proof of your address, such as a copy of a bank statement, utility bill, insurance statement, etc.;
- A copy of your minor dependent's birth certificate;
- A copy of your minor dependent's Social Security card;
- Your minor dependent's full name, including middle initial and generation, such as JR, SR, II, III, etc.;
- Your minor dependent's date of birth; and
- Your minor dependent's previous addresses for the past two years.

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement.