

NOTICE OF DATA EVENT

JULY 29, 2025 - PhyNet Dermatology LLC (“PhyNet”) is providing notice of a data event involving an affiliate, Total Vein & Skin, LLC d/b/a Premier Dermatology Partners (“TVS”). PhyNet provides administrative support to our affiliates, including TVS. While PhyNet is unaware of any actual or attempted identity fraud in relation to the incident, it is providing potentially affected individuals with information about the incident and steps individuals may take to help protect against the possible misuse of their information.

What Happened? On November 7, 2024, PhyNet became aware of suspicious activity relating to an employee’s email account. Upon becoming aware of the activity, PhyNet promptly took steps to secure our email environment and initiated an investigation into the nature and scope of the event. The investigation determined that a limited number of email accounts were compromised, and that information therein may have been viewed or taken. PhyNet undertook a time and labor-intensive review of the files involved to determine what information was involved and to whom it belonged. This review was completed on June 6, 2025, and identified patient information for TVS.

What Information Was Involved? The types of information that may have been impacted varies by individual and may include: full name, address, Social Security number, financial account information, date of birth, medical history information, treatment information, diagnosis information, treating physician, medical record number, and health insurance information.

What We Are Doing. Upon becoming aware of this incident, we immediately took steps to secure our systems and initiated a full investigation. As part of our ongoing commitment to information security, we reviewed our existing policies and procedures, enhanced certain administrative and technical controls, and provided additional security training to reduce the likelihood of a similar future event.

What Affected Individuals Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits and monitoring your free credit reports for suspicious activity and to detect errors. You may also review the information contained in the enclosed *Steps You Can Take to Help Protect Personal Information*.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions or need assistance, please feel free to reach out to our dedicated call center at 877-250-2771 Monday through Friday, 9 am to 9 pm ET, excluding holidays. You may also write to PhyNet at 302 Innovation Drive #400, Franklin, TN 37067.

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 1-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	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your 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, D.C. 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 and the relevant state Attorney General. This notice has not been delayed by law enforcement.