

Dermatology Associates of Concord
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS2403



December 2, 2025

NOTICE OF SECURITY INCIDENT

Dear _____ :

Dermatology Associates of Concord (“DAC”) writes to notify you of an incident that may have impacted your information. This letter provides details of the incident, our response, and steps you may take to help protect against the possible misuse of your information should you feel it is appropriate to do so.

What Happened? On September 19, 2025, DAC identified suspicious activity on certain computer systems within its network. DAC immediately launched an investigation with the help of third-party cybersecurity experts to determine the nature and scope of the activity. The investigation determined that DAC was the victim of a cyber-attack. Specifically, an unauthorized actor gained access to a specific system and copied certain files within DAC’s network from September 18, 2025 to September 19, 2025. Following the investigation, DAC undertook a detailed review of all the impacted files to determine what information was present in these files and to whom it related for purposes of providing notice. While this review is still ongoing, it has been determined that information related to you was impacted in this event. To date, we have seen no evidence of any fraudulent use of any data as a result of this event.

What Information Was Involved? The information potentially impacted by this incident includes your name,

_____. DAC and the third-party cybersecurity experts who conducted the investigation are confident that DAC’s electronic medical record (“EMR”), payment processing, payroll, and email systems were not impacted by this event.

What We Are Doing. DAC takes the confidentiality, privacy, and security of information in its care seriously. Upon discovery of the event, DAC immediately conducted a diligent investigation to confirm the full nature and scope, took prompt steps to ensure security of its environment, and conducted a comprehensive review of the information potentially affected. DAC also notified law enforcement and enhanced its existing security protocols. DAC continues to evaluate its policies and procedures related to data privacy and security. In addition to notifying you and law enforcement, DAC will be notifying applicable state and federal regulators.

As an added precaution, DAC is providing you with access to Single Bureau Credit Monitoring/ Single Bureau Credit Report/ Single Bureau Credit Score services at no charge. These services provide you with alerts for twenty-four (24) months from the date of enrollment if changes occur to your credit file. A notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have. Information on

these services and instructions on how to activate them may be found in the enclosed *Steps You Can Take to Help Protect Your Personal Information*. Please note that you must complete the enrollment process as we are not permitted to enroll you in these services.

What You Can Do. DAC encourages 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 over the next 12 to 24 months. DAC further encourages you to enroll in the complimentary services offered.

For More Information. We understand you may have questions about the incident that are not addressed in this letter. If you have questions, please call 1-800-405-6108 Monday through Friday from 8 a.m. to 8 p.m. EST, excluding holidays. You may also write to DAC at 290 Baker Avenue, Suite N220, Concord, MA 01742.

Sincerely,

Dermatology Associates of Concord

STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

Enroll in Monitoring Services

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: . In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Monitor Your 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 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.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. DAC is located at 290 Baker Avenue, Suite 220N, Concord, MA 01742.

For Massachusetts residents, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov. DAC is located at 290 Baker Avenue, Suite 220N, Concord, MA 01742.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 2 Rhode Island residents that may be impacted by this event.