

Vail Summit Orthopaedics
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998
Via First-Class Mail



August 1, 2025

Notice of Security Incident

Dear [REDACTED]:

Vail Summit Orthopaedics (“Vail Summit”) is writing to inform you of a recent data security incident that has resulted in the unauthorized access to and acquisition of your data. While we are unaware of any fraud or misuse of your data at this time, we are providing you with details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your data. Please be assured Vail Summit takes the protection and proper use of your data very seriously.

What Happened?

On August 6, 2024, Vail Summit learned of suspicious activity in its email environment. Upon discovery, Vail Summit immediately engaged forensic specialists in cybersecurity and data privacy to investigate further. Through this investigation, Vail Summit determined that an unauthorized third party accessed and acquired certain files during this incident. Vail Summit then performed an extensive and comprehensive review of the data to identify what personal information may have been impacted in this incident.

On July 24, 2025, Vail Summit identified the persons whose sensitive information was potentially impacted. Vail Summit’s investigation has found no instances of fraud or identity theft to-date.

What Information Was Involved?

The following data may have been subject to unauthorized access and acquisition: Address, Email, Phone, Date of Birth, Social Security Number, Health Insurance Number, Cost of Medical Treatment or Insurance, Medical Diagnosis/Treatment/Procedure, Medical History/Allergies, Prescription Drugs Taken, Medical Test Results/Images/Vital Signs, Date of Medical Treatment, Medical Treatment Location, Healthcare Provider Name. The information impacted varied by individual.

What We Are Doing?

Data security is one of our highest priorities. Upon detecting this incident, we moved quickly to initiate an investigation. We promptly disabled all relevant accounts and worked with our third-party specialists to confirm the security of our email environment. Again, we take the protection and proper use of personal information seriously.

As part of our ongoing commitment to information privacy and the security of information, we are notifying you of this incident, and we are 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 [REDACTED] months from the date of enrollment if changes were to occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau.

0000102G0500

P

Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

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 [REDACTED]. Please note that the code is case-sensitive and will need to be entered as it appears.

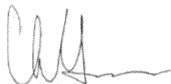
To receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Once enrolled you will have [REDACTED] months of monitoring services. At the end of [REDACTED] months, the services will be deactivated. 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.

For More Information

We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call the dedicated assistance line at 1-833-799-7055 from the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays.

At Vail Summit, we take our responsibilities to protect your personal information very seriously. We are deeply disturbed by this situation and apologize for any inconvenience.

Sincerely,



Chris Greenman
Chief Executive Officer

Steps You Can Take to Help Protect Your Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

| Equifax Security Freeze | Experian Security Freeze | TransUnion Security Freeze |
|---|--|--|
| P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 | P.O. Box 9554 Allen, TX 75013 1-888-397-3742 | P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 |
| https://www.equifax.com/personal/credit-report-services/credit-freeze/ | www.experian.com/freeze/center.html | www.transunion.com/credit-freeze |

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- ◆ Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- ◆ TransUnion (<https://www.transunion.com/fraud-alerts>); or
- ◆ Experian (<https://www.experian.com/fraud/center.html>).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.



00001020280000

P

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud.

For District of Columbia residents, the Attorney General may be contacted at the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov.

For Illinois residents, the Attorney General can be contacted at 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov.

For Maryland residents, you may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491. Vail Summit is located at [Address] and can be reached at [phone number].

For New Mexico residents, state law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You also have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, you may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov. You may also obtain information about steps you can take to prevent identify theft from the North Carolina Attorney General at <https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/>.

For Rhode Island residents, this incident involves 0 individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov.

For Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).