

Exhibit A

Notice of Data Incident

May 8, 2026

On March 10, 2026, Alta Orthopaedics discovered unusual activity on our network and immediately launched an investigation. The investigation determined there was unauthorized access to certain information stored on our network between February 3, 2026 and February 6, 2026. Therefore, we are conducting a comprehensive review of the potentially affected data to determine the types of information potentially affected and to whom it is related. This review is ongoing.

The types of information possibly contained within the affected data may include a patient's name and one or more of the following: address, phone number, email address, Social Security number, driver's license/state ID number, date of birth, billing code, dates of service, reason for visit, cost of treatment, provider name, medical diagnosis, clinical information, treatment location, medical record number, patient account number, and health insurance information.

Through our investigation, we have reset passwords, conduct a thorough investigation, notified law enforcement, and reviewed our policies and procedures related to this incident. We are also providing potentially affected individuals with access to complimentary credit monitoring and identity protection services. If you have questions about this incident or would like to enroll in these services, you may our dedicated call center at 1-877-424-8605, Monday through Friday between 5 am to 5 pm PT, excluding major U.S. holidays. You may also write to us at 511 Bath Street, Santa Barbara, CA 93101.

In general, we encourage potentially affected individuals to remain vigilant against incidents of identity theft and fraud by regularly reviewing credit reports, account statements, and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228.

Individuals have the right to place an initial or extended fraud alert on their credit file at no cost. If an individual is a victim of identity theft, they are entitled to an extended fraud alert lasting seven years. As an alternative to a fraud alert, they have the right to place a credit freeze on their credit report. The credit freeze is designed to prevent credit, loans, and services from being approved without consent. Pursuant to federal law, individuals cannot be charged to place or lift a credit freeze on their credit report.

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

TransUnion

1-800-680-7289

www.transunion.com

Experian

1-888-397-3742

www.experian.com

Equifax

1-888-298-0045

www.equifax.com

Individuals can further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps to protect their personal information by contacting the credit reporting bureaus, the Federal Trade Commission ("FTC"), or their state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. Instances of known or suspected identity theft should also be reported to law enforcement, the state Attorney General, and the FTC.

Exhibit B

Notice of Data Incident

Alta Orthopaedics apprises of a data incident that may have affected individuals' information.

On March 10, 2026, Alta Orthopaedics discovered unusual activity on its network and immediately began an investigation. The investigation determined there may have been unauthorized access to certain information stored on its network between February 3, 2026 and February 6, 2026. Therefore, Alta Orthopaedics conducted a comprehensive review of the data to determine the types of information potentially affected and to whom it is related. On June 24, 2026, Alta Orthopaedics completed its review. The types of information potentially affected may have included a patient's name and one or more of the following: address, telephone number, email address, Social Security number, driver's license/state ID number, other government ID number, passport number, financial account information, login information, date of birth, medical diagnosis, clinical information, MRN, patient account number, date(s) of service, reason for visit, provider name, billing code(s), prescription information, treatment location, cost of treatment, health insurance information, health plan beneficiary number(s), and/or biometric data.

In an abundance of caution, Alta Orthopaedics is providing complimentary credit monitoring and identity protection services to potentially affected individuals. If you have questions about this incident or would like to enroll in these services, you may call their dedicated call center 1-877-424-8605, Monday through Friday between 5 am to 5 pm PT, excluding major U.S. holidays. Individuals are encouraged to remain vigilant against incidents of identity theft and fraud by reviewing credit reports, account statements, and explanation of benefits forms for suspicious activity and to detect errors. Individuals may also place a fraud alert or credit freeze by contacting the credit reporting agencies: TransUnion at 1-800-680-7289; Experian at 1-888-397-3742; Equifax at 1-888-298-0045.

/PRNewswire/ -- July 3, 2026/

SOURCE

Alta Orthopaedics Medical Group, Inc.

Exhibit C



Alta Orthopaedics Medical Group, Inc.
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS4321

39_0011419



<First Name> <Last Name>

<Address>

<City>, <State> <Zip>



July 6, 2026

Notice of Data Breach

Dear <First Name> <Last Name>:

Alta Orthopaedics Medical Group, Inc. writes to notify you of an incident that may affect the privacy of certain information provided to us. This letter includes information about the incident, our response, and resources we are making available to you.

What Happened? On March 10, 2026, we discovered unusual activity on our network and immediately began an investigation. The investigation determined there may have been unauthorized access to certain information stored on our network between February 3, 2026 and February 6, 2026. Therefore, we conducted a review of the data to determine the types of information potentially affected and to whom it related. On June 24, 2026, we completed our review.

What Information Was Involved? The types of information potentially affected may have included your name and the following: [data elements].

What We Are Doing. In response to this incident, we reset passwords, conducted a thorough investigation, notified law enforcement, and reviewed our policies and procedures related to data security. In an abundance of caution, we are also providing you with access to complimentary credit monitoring and identity protection services.

What You Can Do. We encourage you to enroll in the services that we are making available to you. Information about how to enroll in these services and additional resources available to you are included in the attached *Steps You Can Take to Help Protect Your Information*. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports, account statements, and explanation of benefits forms for suspicious activity and to detect errors.

For More Information. If you have any questions about this incident, you may contact our dedicated call center at 1-877-424-8605, Monday through Friday between 5 am and 5 pm PT, excluding major U.S. holidays or write to us at 511 Bath Street, Santa Barbara, CA 93101.

We sincerely regret any concern this incident may cause you. The privacy and security of information is important to us, and we will continue to take steps to protect information in our care.

Sincerely,

Alta Orthopaedics Medical Group, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Credit Monitoring Services

In response to the incident, we are providing you with access to credit monitoring services at no charge. These services provide you with alerts for [12/24] months from the date of enrollment when changes occur to your credit file. This 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 or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company.

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: **[code]**. 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. 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, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You 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, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you 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 your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

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

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

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
---	---	--

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (“FTC”), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. 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; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. Alta Orthopaedics Medical Group, Inc. may be contacted at 511 Bath Street, Santa Barbara, CA 93101.

For New Mexico residents, you 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 bureaus 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 violator. 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 by visiting 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, 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.

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, you have the right to obtain any police report filed in regard to this incident. There are 4 Rhode Island residents impacted by this incident.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 400 6th Street, NW, Washington, D.C. 20001; 202-442-9828, and <https://oag.dc.gov/consumer-protection>. Alta Orthopaedics Medical Group, Inc. may be contacted at 511 Bath Street, Santa Barbara, CA 93101.