

## EXCELSIOR ORTHOPAEDICS, LLP PROVIDES NOTICE OF DATA SECURITY INCIDENT

Amherst, NY – January 3, 2025 – Excelsior Orthopaedics, LLP (“Excelsior”) is writing to inform you of a data security incident that resulted in the compromise of sensitive or personal information pertaining to current and former patients and employees of Excelsior and its related entities, including Buffalo Surgery Center and Northtowns Orthopaedics. In an abundance of caution, we are offering free credit monitoring and identity theft protection services to affected individuals. Please see additional information below, including details about the incident, instructions for enrolling in credit monitoring services, steps we are taking in response, and resources to help you protect against the potential misuse of your information.

**What Happened?** On June 23, 2024, Excelsior detected unusual activity on its network and discovered that it was the victim of a data security incident. Upon discovery of this incident, Excelsior immediately took steps to contain the intrusion and engage a specialized third-party cybersecurity firm to help secure the environment and conduct a comprehensive forensic investigation into the nature and scope of the incident. Excelsior also engaged outside data mining experts to conduct a thorough analysis of the compromised data and identify affected individuals. In August 2024, with the data mining process ongoing, Excelsior mailed an initial wave of notices to a small population of affected individuals and reported the incident to the U.S. Department of Health and Human Services and the Office for Civil Rights. The bulk of data mining was completed in December 2024, which identified additional individuals for purposes of notification. Excelsior mailed a second wave of notices to patients on December 31, 2024. Efforts to identify affected individuals are ongoing, and any remaining affected individuals will be notified via first class mail as they are identified.

**What Information Was Involved?** Excelsior is still in the process of identifying the individuals and data impacted as a result of this incident. The types of data compromised include demographic information, driver’s license number, medical information, health insurance information, and financial information. In limited number of instances, an individual’s Social Security number may have been impacted. Please note, compromised information varies for each individual and additional information about impacted data can be found in the **“What Information Was Involved”** section of the notice letters mailed to affected individuals.

**What Excelsior is Doing:** Since the discovery of the incident, Excelsior has taken steps to mitigate the risk of future issues. Specifically, Excelsior has engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. In addition, Excelsior has taken steps to enhance existing security measures and prevent similar events from occurring in the future, including deploying new security tools to augment its security platform, redesigning key system and business processes, and implementing enhanced system alerts to reduce response times. Excelsior is also improving security training and awareness campaigns designed to educate employees and business

partners on cybersecurity threats. Excelsior is committed to ensuring the privacy and security of all personal information in our care, and we will continue to take steps to mitigate the risk of future harm. Excelsior is offering complimentary credit monitoring and identity theft protection services to affected individuals whose personal information was impacted. Affected individuals were mailed notices containing information on how to enroll in the credit monitoring services.

**What You Can Do:** Excelsior encourages 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 *Steps You Can Take to Help Protect Your Information* below to learn more about how to protect against the possibility of information misuse.

If you have any questions or concerns not addressed in this letter, please call **1-833-531-2298** [toll free] Monday through Friday, during the hours of 8 a.m. and 8 p.m. EST (excluding U.S. national holidays). We sincerely regret any inconvenience this matter may cause and remain dedicated to ensuring the privacy and security of all information in our control.

Sincerely,



David Uba

CEO

Excelsior Orthopaedics, LLP

### 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](http://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.

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

**Experian**

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742

[www.experian.com/fraud/  
center.html](http://www.experian.com/fraud/center.html)

**TransUnion**

P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289

[www.transunion.com/  
fraud-alerts](http://www.transunion.com/fraud-alerts)

**Equifax**

P.O. Box 105069  
Atlanta, GA 30348  
1-800-525-6285

[https://www.equifax.com/personal/  
credit-report-services/credit-fraud-  
alerts/](https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/)

**Monitoring:** You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

**Security Freeze:** You 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:

**Experian**

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742

[www.experian.com/freeze/  
center.html](http://www.experian.com/freeze/center.html)

**TransUnion**

P.O. Box 160  
Woodlyn, PA 19094  
1-888-909-8872

[www.transunion.com/  
credit-freeze](http://www.transunion.com/credit-freeze)

**Equifax**

P.O. Box 105788  
Atlanta, GA 30348-5788  
1-888-298-0045

[https://www.equifax.com/personal/  
credit-report-services/credit-freeze/](https://www.equifax.com/personal/credit-report-services/credit-freeze/)

**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. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

**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](http://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. Instances of known or suspected identity theft should also be reported to law enforcement.

---

**For residents of Iowa:** State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

---

**For residents of Massachusetts:** It is required by state law that you are informed of your right to obtain a 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 residents of New Mexico:** State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. 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 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](http://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 residents of Oregon:** State law advises you to report any suspected identity theft to

law enforcement, including the Attorney General, and the Federal Trade Commission.

---

**For residents of Rhode Island:** It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

---

**For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island:** You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

**Federal Trade Commission - Consumer Response Center:** 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT [438-4338]; [www.identitytheft.gov](http://www.identitytheft.gov)

**Arizona Office of the Attorney General Consumer Protection & Advocacy Section,** 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

**Colorado Office of the Attorney General Consumer Protection** 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 [www.coag.gov](http://www.coag.gov)

**District of Columbia Office of the Attorney General – Office of Consumer Protection:** 400 6th Street, NW, Washington, DC 20001; 202-727-3400; [www.oag.dc.gov](http://www.oag.dc.gov)

**Illinois office of the Attorney General -** 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; [www.illinoisattorneygeneral.gov](http://www.illinoisattorneygeneral.gov)

**Maryland Office of the Attorney General - Consumer Protection Division:** 200 St. Paul Place, 16<sup>th</sup> floor, Baltimore, MD 21202; 1-888-743-0023; [www.oag.state.md.us](http://www.oag.state.md.us)

**New York Office of Attorney General - Consumer Frauds & Protection:** The Capitol, Albany, NY 12224; 1-800-771-7755; <https://ag.ny.gov/consumer-frauds/identity-theft>

**North Carolina Office of the Attorney General - Consumer Protection Division:** 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; [www.ncdoj.com](http://www.ncdoj.com)

**Rhode Island Office of the Attorney General - Consumer Protection:** 150 South Main St., Providence RI 02903; 1-401-274-4400; [www.riag.ri.gov](http://www.riag.ri.gov)

---