Jennifer S. Stegmaier
312.821.6167 (direct)
Jennifer.Stegmaier@wilsonelser.com

Via Online Portal

September 2, 2025

Attorney General Mike Hilgers
Office of the Attorney General
Consumer Affairs Response Team
2115 State Capitol
Lincoln, NE 68509

Re: Supplemental Notice of Data Incident Involving Excelsior Orthopaedics, LLP

Dear Attorney General Hilgers:

Wilson Elser Moskowitz Edelman and Dicker, LLP ("Wilson Elser") represents Excelsior Orthopaedics, LLP ("Excelsior"), a healthcare company that specializes in orthopaedic treatment with 10 locations across western New York and is headquartered at 3925 Sheridan Drive, Amherst, NY 14226. Please accept this as Excelsior's supplemental notice regarding the cybersecurity incident it discovered on June 23, 2024 (hereinafter, the "incident"). Excelsior takes the security and privacy of the information within its control very seriously and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to provide an update as to the nature of the incident, what information may have been compromised, the number of Nebraska residents being notified, and the steps that Excelsior has taken in response to the incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services.

1. Nature of the Incident

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 engaged 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.

Initial results of the forensic investigation indicated that the incident resulted in the compromise of data relating to current and former patients and employees of Excelsior and its related entities, including Buffalo Surgery Center and Northtowns Orthopedics. In light of these findings, Excelsior, with the assistance of outside data mining experts, conducted a thorough analysis of the data contained in the compromised system to identify the potentially affected individuals and types of information that may have been compromised. In an abundance of caution, as the forensic investigation and data mining were ongoing, Excelsior began providing notice to the potentially affected individuals in waves as information became available.

The forensic investigation concluded on or about October 22, 2024, and determined that there was unauthorized access to Excelsior's computer system from June 18, 2024, to June 27, 2024. Excelsior completed its review of the impacted systems on or about July 30, 2025. During Excelsior's review process it provided notice to the potentially impacted individuals on a rolling basis. Excelsior also mailed supplemental notification letters to some individuals for whom it discovered additional personally identifiable information in the impacted systems which contained new data elements that were not previously identified in their original notification letters. Individual notification letters were mailed to potentially impacted individuals *via* United States first class mail in waves on July 25, 2024, December 31, 2024, January 2, 2025, February 11, 2025, and August 26, 2025.

2. Number of residents affected.

Excelsior identified and notified a total of 14 Nebraska residents (in all waves) whose information may have been impacted as a result of the incident. Notification letters were mailed to the potentially impacted individuals in waves beginning on June 18, 2024, and concluding on August 26, 2025. A sample notification letter is enclosed hereto as **Exhibit A**.

3. Steps taken in response to the Incident.

Excelsior is committed to ensuring the security and privacy of all personal information under its control and is taking steps to prevent a similar incident from occurring in the future. After discovering the incident, we acted quickly to contain the intrusion and secure our environment by disconnecting all external access to the network, isolating suspect equipment, and changing credentials across the organization to safeguard user and administrative system accounts. In an effort to prevent similar incidents from occurring in the future, we have worked with outside cybersecurity experts to implement a number of security enhancements that include deploying new security tools, redesigning key system and business processes, partnering with a first-in-class managed security provider, and implementing enhanced internal security awareness campaigns and system alerts. We have also reported this incident to the FBI and cooperated with law enforcement investigations. Excelsior has and will continue to take steps to mitigate the risk of future incidents and prevent harm.

Excelsior also offered twelve (12) months of complimentary credit monitoring and identity theft restoration services through CyberScout, a TransUnion company, to all affected residents to help protect their identity. Additionally, Excelsior provided guidance on how to better protect against

identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

4. Contact information

Excelsior remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Jennifer.Stegmaier@wilsonelser.com or 312-821-6167.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Jennifer S. Stegmaier

EXHIBIT A