WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

August 6, 2021

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via First Class Mail

Attorney General of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Re: Notice of Cybersecurity / Data Privacy Incident
Client: Southern Orthopaedic Surgeons
File No.: 15991.00879

Dear Attorney General:

Wilson Elser represents Southern Orthopaedic Surgeons ("Southern"), an orthopedic surgical practice with multiple locations throughout the state of Alabama. Southern was impacted in a cybersecurity incident that compromised an employee's business email account. This letter contains more information about the incident and steps Southern has taken in response.

1. **Nature of the incident.**

On October 20, 2020, Southern discovered that an employee's email account had been accessed by an unknown individual. After learning of the incident, Southern engaged outside forensic experts to determine whether the incident resulted in the exposure of sensitive information. The forensic experts completed their investigation in early February. Southern then engaged a data review team to determine which individuals it needed to notify. The forensic experts completed their investigation in early February. On June 11, 2021, the data mining project confirmed that Personally Identifiable Information ("PII") and Protected Heath Information ("PHI") may have been exposed as a result of the unauthorized email compromise.

The forensic investigation, along with the data mining project confirmed that PII and PHI such as full names in combination with one or more of the following may have been compromised: social security numbers, driver's license numbers, date of birth, clinical information, doctor's notes and other treatment information.

2. **Number of New Hampshire residents affected.**

One (1) New Hampshire resident was potentially affected by this incident. Incident notification letters are set to be mailed out on August 9, 2021 via First Class Mail. A sample copy of the Incident notification letter mailed to potentially affected resident(s) is included with this letter at **Exhibit A**.

3. **Steps taken.**

At this time, there is no evidence that any information has been misused as a result of this incident. Southern has taken steps to further safeguard data in the future - including but not limited to implementing policies prohibiting employees from emailing patient information, updating the

firewall protections to include 24 hour monitoring and requiring regular password resets. Southern is also offering complimentary credit monitoring to the affected individuals who had sensitive data, such as Social Security numbers and Driver's License numbers, exposed as a result of the incident.

4. Contact information.

Southern 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 Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

Enclosure

EXHIBIT A

Southern Orthopaedic Surgeons LLC

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notice of Security Incident

Dear <<Name 1>>:

Southern Orthopaedic Surgeons ("Southern") is dedicated to orthopaedic care of its patients. Out of an abundance of caution, we are writing to inform you of a data security incident that may have resulted in the exposure of some of your personal data. Please know we take the security of your information very seriously. Southern sincerely apologizes for any inconvenience this incident may cause you. This letter contains information about the incident and steps you can take to further protect your information.

What Happened:

On October 20, 2020, Southern discovered that one employee's email account had been accessed by an unknown individual. Upon discovery of the incident, Southern promptly engaged independent forensic experts and data review team to determine whether the incident resulted in the exposure of sensitive information. On June 11, 2021, the data review confirmed that protected heath information of Sothern's patients may have been exposed as a result of the unauthorized email compromise. Thereafter, Southern promptly began a thorough internal review to identify potentially impacted individuals whose information may have been exposed during the period of unauthorized access. The internal investigation was necessary in order to identify the individuals whose information may have been impacted by the incident.

What Information Was Involved:

Based on the internal investigation, the unauthorized individual may have had access to one or more of the following data elements: your name, Social Security number, driver's license number, date of birth, clinical information, doctor's notes, and other limited treatment information may have been viewed by an unauthorized individual. At this time, Southern has no reason to believe that any patient information has been misused as a result of this incident.

What We Are Doing:

In response to this incident, Southern has taken the following steps: implemented policies prohibiting employees from emailing patient information, updating the firewall protections to include 24-hour monitoring and requiring regular password resets.

What You Can Do:

Southern recommends that you continue to remain vigilant in monitoring your personal information. Southern refers you to the *Additional Important Information* section of this letter, which provides you with further information to obtain your credit report, place fraud alerts and freeze your credit.

For more information:

The protection of your information is our top priority, and Southern sincerely regrets any inconvenience that this matter may cause you. If you have any questions, or require additional information please call the following toll-free number: 800-397-1203. Representatives are available to assist you from 9:00 a.m. to 9:00 p.m. Eastern Time, Monday through Friday.

Sincerely,

Jenna Roton

Jenna Roton

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon,* and *West Virginia*:

It is required by state laws to inform you that 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.

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 *Oregon*:

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Arizona, Colorado, District of Columbia, Maryland, Rhode Island, Illinois, New York, and North Carolina:

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.

Maryland Office of the Attorney General Consumer Protection Division 200, St. Paul Place Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection 150 South Main Street, Providence RI 02903; 1-401-274-4400; www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001; 1-877-566-7226; www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.ftc.gov/idtheft

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

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203; 1-720-508-6000; www.coag.gov

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

Illinois Office of the Attorney General Consumer Protection Division 100 W Randolph St., Chicago, IL 60601; 1-800-243-0618; www.illinoisattorneygeneral.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

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft

For residents of all states:

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 section.

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

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
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.