July 8, 2022

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

***Via Online Portal:***

**Attorney General Aaron Frey**
Office of the Attorney General
Attn: Security Breach Notification
Department of Professional & Financial Regulation
Bureau of Consumer Credit Protection
35 State House Station
Augusta, Maine 04333

**Re: Cybersecurity Incident Involving North American Spine Society**

Dear Attorney General Frey:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents The North American Spine Society ("NASS"), a medical society for health care professionals who specialize in spine care, with respect to a recent data privacy incident that was first discovered by NASS on February 13, 2022 (hereinafter, the "Incident"). NASS takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of Maine residents being notified, and the steps that NASS 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 February 13, 2022, NASS was subject to a data security incident that impacted its servers. Upon discovery of the incident, NASS promptly engaged a team of cyber security professionals to assist with the recovery of its business services, and to conduct a forensic investigation to determine the scope and the overall impact of the incident. Based on the limited available forensics artifacts, the investigation was inconclusive as to whether any sensitive data was subject to unauthorized acquisition. As such, NASS notified all potentially affected individuals out of an abundance of caution.

Although NASS is unaware of any fraudulent misuse of information, it is possible that individuals' name, address, date of birth, check information, financial account information, social security

number, passport number, credit card information, medical ID and/or driver's license number may have been exposed as a result of this unauthorized activity.

As of this writing, NASS has not received any reports of related identity theft since the date of the incident (February 13, 2022 to present).

**2. Number of Maine residents affected.**

A total of 17 Maine residents have been potentially affected by this incident. Notification letters to individuals were mailed on July 8, 2022 by first class mail. A sample copy of the notification letter is included with this letter under **Exhibit A**.

**3. Steps taken in response to the Incident.**

NASS is committed to ensuring the security and privacy of all personal information in its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, NASS moved quickly to investigate and respond to the Incident, assessed the security of its systems, and notified the potentially affected individuals. In response to the Incident, NASS deleted all of the systems and rebuilt from the nearest set of backups that were scanned and shown as unaffected.

Although NASS is not aware of any actual or attempted misuse of the affected personal information, NASS offered 12 months of complimentary credit monitoring and identity theft restoration services through Cyberscout to all individuals to help protect their identity. Additionally, NASS 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**

The North American Spine Society 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

# EXHIBIT A

<Return Name>
<Return Address>
<City> <State> <Zip>

<FirstName> <LastName>
<Address1>
<Address2>
<City>, <State> <Zip>

<<Date>>

**Notice of Data Breach**

Dear <<First Name>><<Last Name>>,

North American Spine Society ("NASS") is writing to inform you of a recent cybersecurity incident (the "Incident") that involved some of your personal information. This letter contains details about the Incident, steps we have taken in response, and services we are making available to you.

**What Happened?**

On or about February 13, 2022, NASS learned it had become a victim of a cybersecurity incident which may have resulted in unauthorized access to your Personally Identifiable Information ("PII"). After learning about the potential unauthorized access, NASS immediately launched an investigation to review the impacted servers in order to learn more about the scope and extent of the incident, and whether PII may have been exposed.

The investigation completed on March 18, 2022, and confirmed an unauthorized individual accessed NASS's servers, but there was no evidence sensitive data was accessed. On June 14, 2022, NASS identified the specific individuals and the types of information that were stored on the impacted servers.

**What Information Was Involved?**

Upon further review, NASS discovered that personally identifiable information, such as your full name in combination with <<data elements>> may have been impacted. There was no evidence your personal information was accessed; however we are notifying you out of an abundance of caution.

**What We Are Doing**

NASS takes the security of your personal information very seriously, and has taken steps to prevent a similar event from occurring in the future. In order to help relieve concerns and restore confidence following this incident, we are providing you with access to Single Bureau Credit Monitoring* services at no charge. These services provide you with alerts for twelve (12) 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. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a company specializing in fraud assistance and remediation services. The protection of your information is a top priority, and we sincerely regret any concern or inconvenience that this incident may cause you. We remain dedicated to maintaining the security and protection of your information.

To enroll in Credit Monitoring* services at no charge, please log on to **https://www.xxx.com** and follow the instructions provided. When prompted please provide the following unique code to receive services: **<<unique code>>**

## What You Can Do

Although we are not aware of any instances of misuse of personal information, we recommend that you take advantage of the complimentary credit monitoring and identity theft protection services out of an abundance of caution. Instructions on how to do so are included in the materials enclosed with this letter. We encourage you to remain vigilant and review the enclosed addendum outlining additional steps you can take to protect your personal information. If you have any questions or want to enroll in the complimentary identity monitoring services, please follow the instructions below.

## For More Information

NASS recognizes that you may have questions not addressed in this letter. If you have additional questions, please call 1-800-405-6108 (toll free) during the hours of 8:00 am to 8:00 pm Eastern, Monday through Friday (excluding U.S. national holidays).
NASS sincerely regrets any inconvenience or concern that this matter may cause, and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

NASS
ADVANCING GLOBAL SPINE CARE

## ***Additional Important 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.

**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** | **TransUnion** | **Equifax** |
|---|---|---|
| P.O. Box 9554 | P.O. Box 2000 | P.O. Box 105069 |
| Allen, TX 75013 | Chester, PA 19016 | Atlanta, GA 30348 |
| 1-888-397-3742 | 1-800-680-7289 | 1-800-525-6285 |
| www.experian.com/fraud/center.html | www.transunion.com/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** | **TransUnion** | **Equifax** |
|---|---|---|
| P.O. Box 9554 | P.O. Box 160 | P.O. Box 105788 |
| Allen, TX 75013 | Woodlyn, PA 19094 | Atlanta, GA 30348-5788 |
| 1-888-397-3742 | 1-888-909-8872 | 1-888-298-0045 |
| www.experian.com/freeze/center.html | www.transunion.com/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, 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 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

**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

**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

**Illinois office of the Attorney General -** 100 West Randolph Street**,** Chicago, IL 60601**;** 1-866-999-5630**;** www.illinoisattorneygeneral.gov

**Maryland Office of the Attorney General -** Consumer Protection Division**:** 200 St. Paul Place**,** 16th floor, Baltimore, MD 21202; 1-888-743-0023; 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

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