

December 2, 2021

Ryan M. Cook
601.499.8087 (direct)
Ryan.Cook@wilsonelser.com

Via electronic-mail: DOJ-CPB@doj.nh.gov; AttorneyGeneral@doj.nh.gov

Attorney General John M. Formella

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Re: Our Client : Boulder Neurosurgical and Spine Associates
Matter : Data Incident detected September 21, 2021
Wilson Elser File # : 16516.01656

Dear Attorney General Formella:

We represent Boulder Neurosurgical and Spine Associates (“BNA”) located at 4743 Arapahoe Ave No. 202, Boulder, Colorado 80303, with respect to a potential data security incident described in more detail below. BNA provides care to patients at its office in Boulder, Colorado. Notification has been provided to potentially impacted individuals.

1. Nature of security incident.

On or about September 21, 2021, BNA experienced a compromise to one of its business email accounts. BNA quickly engaged cybersecurity experts and a leading incident response team to secure the subject email account, assess the extent of the unauthorized activity, and remediate any damage caused by the incident.

BNA has found no evidence that patient information was specifically accessed or misused, however the investigation revealed that there was unauthorized access to an email account which may have contained PHI. BNA made the decision to notify all of the clinic’s patients of this incident out of an abundance of caution.

As of this writing, we have not received any reports of related identity theft since the date of the incident (September 21, 2021 to present).

2. Number of New Hampshire residents affected.

Three (3) New Hampshire residents were potentially affected by the data security incident. Notification letters to those individuals were mailed on November 24, 2021, via regular mail. A copy of the notification letter is included with this letter.

3. Steps you have taken or plan to take relating to the incident.

Upon discovering this incident, BNA immediately launched an investigation to determine the nature and scope of the event, as well as whose data may potentially be affected. BNA has mailed written notice to all of the clinic's patients out of an abundance of caution. This notice includes guidance on how to better protect against identity theft and fraud, 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 encouragement to report attempted or actual identity theft and fraud. As an added precaution, BNA arranged to have IDX provide the affected consumers twelve (12) months of credit monitoring and identity restoration services at no cost to the individual. BNA is also providing notice of this event to other state and federal regulators, as well as notice to multiple media outlets. In addition, BNA has notified the three major credit reporting agencies (Equifax, TransUnion, Experian) of the incident.

4. Contact information.

Boulder Neurosurgical and Spine Associates is committed to the protection and security of its patient records. If you have any questions or need additional information, please do not hesitate to contact me at Ryan.Cook@WilsonElser.com or (601) 499-8087.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Ryan M. Cook, Esq.

Copy: Michael E. Kar, Esq. (Wilson Elser LLP)

Enclosure: *Sample Notification Letter*

P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-820-0974
Or Visit:
[https://app.idx.us/account-
creation/protect](https://app.idx.us/account-creation/protect)
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>

November 24, 2021
Via First-Class Mail

Notice of Data Breach

Dear <<FIRST NAME>> <<LAST NAME>>,

The privacy and security of our patients' data is a responsibility that Boulder Neurosurgical and Spine Associates ("BNA") takes seriously. We are writing in order to inform you of an incident that could have exposed your protected health information ("PHI") and want to provide you with resources you can use to protect your information.

What Happened and What Information was Involved:

On September 21, 2021, BNA detected a compromise to one of its business email accounts. BNA quickly engaged cybersecurity experts and a leading incident response team to secure the subject email account, assess the extent of the unauthorized activity, and remediate any damage caused by the incident. A third-party IT forensics firm also launched an investigation to determine what, if any, information could have been compromised in the incident.

Although we have found no evidence that your information was specifically accessed or misused, the investigation confirmed that there was unauthorized access to an email account which may have contained your personal health information. This may have included your name, date of birth, and medical records. Addresses were social security numbers were not compromised in the incident.

What We Are Doing:

Upon detecting suspicious activity on our network, we moved quickly to investigate and respond. This included confirming the security of our email environment and notifying impacted patients of this incident. As part of BNA's ongoing commitment to the security of information, we have reviewed and enhanced our data security policies and procedures in order to reduce the likelihood of a similar event in the future. We are providing additional training and education for our staff.

Although there is no evidence that any of the information involved has been or will be misused, we value the safety of your personal information and are offering complimentary credit monitoring and identity theft protection services through IDX. IDX's services include: <<Service Length>> months of credit and CyberScan monitoring and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do:

We encourage you to remain vigilant against incidents of identity theft and fraud by enrolling in this free identify theft protection and credit monitoring. Contact IDX with any questions and to enroll in these services by calling 1-833-820-0974 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX is available Monday through Friday 6am to 6pm Pacific Time. Please note the deadline to enroll is February 24, 2022.

Again, at this time, there is no evidence that your information has been taken or misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Enclosed you will find additional information regarding the resources available to you, and the steps that you can take to further protect your personal information.

For More Information:

If you have additional questions, please call IDX at the number provided above.

BNA values the privacy and importance of your personal health data, and we apologize for any inconvenience or concern that this incident has caused.

Sincerely,

Boulder Neurosurgical and Spine Associates

(Enclosure)

Additional 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.

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 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 www.transunion.com/credit-freeze
---	---	--

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 listed above.

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

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. 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. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

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 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 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 North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.

For New York residents, the Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, and <https://ag.ny.gov/>.

For Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 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.
