

March 14, 2023

VIA ELECTRONIC MAIL

Attorney General Anthony G. Brown
Maryland Attorney General's Office
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-Mail: Idtheft@oag.state.md.us

Re: Notification of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith and Prophete, LLP ("Constangy") represents the Bone & Joint Clinic S.C. ("Bone & Joint") of Wausau, Wisconsin regarding a recent data security incident described below. The purpose of this letter is to notify you of the incident in accordance with the Maryland data breach notification law.

1. Nature of the Security Incident

On January 16, 2023, Bone & Joint experienced a network disruption and immediately began investigating the matter with the assistance of cybersecurity experts. On January 27, 2023, the investigation determined that personal information may have been acquired without authorization during the incident.

2. Type of Information and Number of Maryland Residents Affected

Bone & Joint notified fourteen (14) residents of Maryland of this data security incident via U.S. mail on March 7, 2023. The information accessed and potentially acquired by an unknown person may have included names, dates of birth, Social Security numbers, home addresses, phone numbers, health insurance information, and diagnosis and treatment information.

3. Steps Taken Relating to the Incident

Bone & Joint has offered all individuals complementary identity protection services through IDX, including dark web monitoring, up to \$1 million in identity fraud loss reimbursement insurance, fully managed identity theft recovery services, and access to a call center for ninety days. Additionally, Bone & Joint has offered all individuals whose Social Security numbers may have been affected twelve months of complimentary credit monitoring services through IDX.

4. Contact Information

Bone & Joint remains dedicated to protecting the personal information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at 503.459.7707 or by email at SHoar@constangy.com or Amir Goodarzi at 215.801.1108 or AGoodarzi@constangy.com.

Sincerely,



Sean B. Hoar

Partner & Chair, Cybersecurity & Data Privacy Team

Enc.: Sample Consumer Notification Letter



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

To Enroll, Please Call:
(833) 758-8873
Or Visit:
<https://response.idx.us/bonejoint>
Enrollment Code: <<ENROLLMENT>>

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

March 7, 2023

Subject: Notice of Data <<Variable Text 2>>

Dear <<FIRST NAME>> <<LAST NAME>>:

I am writing to inform you of a data security incident that may have affected your personal information. At Bone & Joint Clinic, S.C. ("Bone & Joint"), we take the privacy and security of personal information very seriously. This is why we are informing you of the incident, providing you with steps you can take to protect your personal information, and offering you complimentary credit monitoring and identity protection services.

What Happened? On January 16, 2023, Bone & Joint experienced a network disruption and immediately initiated an investigation of the matter. We engaged cybersecurity experts to assist with the process. The investigation determined that certain administrative and medical files may have been acquired without authorization. After a thorough review of those files, on or about January 27, 2023, some of your personal information was identified as being contained within the potentially affected data.

What Information Was Involved? The information may have involved your name, date of birth, Social Security number, home address, phone number, health insurance information, and diagnosis and treatment information.

What Are We Doing? As soon as Bone & Joint discovered the incident we took the steps described above. We also implemented measures to enhance network security and minimize the risk of a similar incident occurring in the future. We also notified the Federal Bureau of Investigation and will provide whatever cooperation may be necessary to hold the perpetrators accountable. In addition, we are offering you complimentary credit monitoring and identity protection services through IDX, a leader in consumer identity protection. These services include <<12/24>> months of credit monitoring, identity protection through CyberScan monitoring, a \$1,000,000 identity theft insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is affected.

What Can You Do? We recommend that you review and implement the guidance included with this letter about how to protect your information. We also encourage you to enroll in the services offered to you through IDX by contacting (833) 758-8873 or going to <https://response.idx.us/bonejoint> and using the enrollment code provided above. Please note the deadline to enroll is June 7, 2023.

For More Information: Further information about how to help protect your personal information appears on the

Bone & Joint Clinic, S.C.
225000 Hummingbird Road, Suite 11
Wausau, WI 54401

following page. If you have questions or need assistance, please call (833) 758-8873 Monday through Friday from 8 am - 8 pm Central Time or go to <https://response.idx.us/bonejoint>. We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Brent Turner", with a long horizontal flourish extending to the right.

Brent Turner
Chief Executive Officer
Bone & Joint Clinic, S.C.

Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

**Washington D.C. Attorney
General**

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf.