



LEWIS BRISBOIS BISGAARD & SMITH LLP

Robert L. Slaughter III
633 W. 5th Street, Suite 4000
Los Angeles, CA 90071
Robert.Slaughter@lewisbrisbois.com
Direct: 213.680.5028

February 27, 2020

VIA E-MAIL

Gordon MacDonald, Attorney General
Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

We represent Tennessee Orthopaedic Alliance (“TOA”), an orthopaedic surgery group located in Nashville and Middle Tennessee. This letter is being sent because five (5) New Hampshire residents may have been affected by a recent data security incident and are being notified in connection therewith. Of those, one (1) resident is being notified pursuant to N.H. Rev. Stat. §§ 359-C:19, C:20, C:21, because the resident’s personal information may have been impacted, which may have involved unauthorized access to one (1) resident’s name and Social Security number.

On October 18, 2019, TOA detected unusual activity in an employee’s email account. TOA immediately took measures to secure its email system and launched an investigation with the assistance of a digital forensics firm to help determine what occurred and whether personal information was accessed without authorization. Based on the digital forensic firm’s findings, it was determined that a very limited number of TOA employee email accounts were subject to unauthorized access between approximately August 16 and October 14, 2019. The unauthorized access was limited to information transmitted via email and did not affect any other information systems. In response, TOA launched a data review project to identify whether personal information within those accounts may have been accessed without authorization. TOA also reported the incident to law enforcement.

On January 3, 2020, the investigation revealed that data containing individuals’ personal information within one or more email accounts may have been affected. TOA then worked diligently to identify up-to-date address information required to notify potentially impacted individuals. On February 14, 2020, TOA provided notification of the incident to the U.S. Department of Health and Human Services’ Office for Civil Rights (“OCR”), pursuant to the HIPAA Breach Notification Rule.

February 27, 2020

Page 2

TOA initially issued notices via the attached sample letter, or a substantially similar version, on February 14, 2020, at which time available information did not identify that the personal information of New Hampshire residents was impacted. On February 24 and 26, 2020, TOA issued remaining notices upon confirming additional addresses, including to one (1) New Hampshire resident whose personal information may have been impacted. TOA is offering twelve (12) months of complimentary credit monitoring and identity protection services through Kroll to individuals whose Social Security numbers were potentially impacted.

Please contact me should you have any questions.

Sincerely,

/s/ Robert L. Slaughter III

Robert Slaughter of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Consumer Notification Letter

LEWIS BRISBOIS BISGAARD & SMITH LLP

www.lewisbrisbois.com



TENNESSEE ORTHOPAEDIC ALLIANCE

<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip>>

Re: Notification of Data Security Incident

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

We are writing to inform you of a data security incident experienced by Tennessee Orthopaedic Alliance (“TOA”) that may have affected your personal or health information. TOA takes the privacy and security of patient information very seriously and deeply regrets any concern that this incident may cause. We are writing to notify you of this incident, to offer you complimentary identity monitoring services, and to inform you about steps that can be taken to help monitor your information.

What Happened? On October 18, 2019, TOA discovered unusual activity in an employee’s email account. TOA immediately took steps to secure its email system and launched an investigation with the assistance of a leading digital forensics firm to determine whether additional email accounts may have been impacted and whether any personal information was accessed or acquired without authorization. Through this investigation, TOA learned that an email account belonging to a second employee may have been impacted as well. The two email accounts were subject to unauthorized access by an unknown party between August 16 and October 14, 2019. On January 3, 2020, our investigation determined that your information was contained in the impacted accounts and therefore may have been viewed or accessed without authorization, though the investigation could not conclude definitively whether your information was actually accessed or acquired. TOA then worked to identify up-to-date address information required to notify potentially impacted individuals.

Please note that this incident was limited to information transmitted via email and did not affect any other information systems. Moreover, we have no evidence to suggest your personal information has been misused. Nonetheless, out of an abundance of caution, TOA is notifying you of this incident and providing you with information about steps you can take to help safeguard your information.

What Information Was Involved? The information may have included your name, contact information (such as address, phone number and email address), date of birth, Social Security number, health insurance information, treatment or diagnostic information (including codes), and/or treatment cost information.

What We Are Doing. As soon as we discovered this incident, we took the measures referenced above. We also implemented enhanced security measures in order to better safeguard all personal information in our possession and to help prevent a similar incident from occurring in the future. In addition, we reported this matter to the Federal Bureau of Investigation and will provide whatever assistance is necessary to hold the perpetrators of this incident accountable. Additionally, out of an abundance of caution, we are providing you with information about steps you can take to help safeguard your information and complimentary identity monitoring services through Kroll, a global leader in risk mitigation and response. These services include Credit Monitoring, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

What You Can Do. We recommend that you review the guidance included with this letter about how to monitor your personal information. In addition, we recommend that you activate the complimentary identity monitoring services being offered through Kroll. Activation instructions and a description of the services being provided are included with this letter.

For More Information. If you have questions or need assistance, please contact Kroll at 1-844-936-0059, Monday through Friday from 8 a.m. to 5:30 p.m. Central Time. Our representatives are fully versed on this incident and can answer any questions you may have regarding how to help safeguard your personal information.

Thank you for your patience through this incident. We take your trust in us and this matter very seriously. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Rob Simmons". The signature is fluid and cursive, with a long horizontal stroke at the end.

Rob Simmons
Chief Executive Officer
Tennessee Orthopaedic Alliance

Steps You Can Take to Further Protect Your 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 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 can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

TransUnion P.O. Box 1000 Chester, PA 19016 1-877-322-8228 www.transunion.com	Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	Equifax P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285 www.equifax.com	Free Annual Report P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 annualcreditreport.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 one (1) 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. 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. There is no charge to place, lift or remove the security freeze. 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 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. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

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 oag.state.md.us 1-888-743-0023	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 401-274-4400
---	---	---	--

You also have certain rights under the Fair Credit Reporting Act (FCRA), including: 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 others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

As referenced above, we have secured the services of Kroll to provide identity monitoring services at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your services¹ include Credit Monitoring, \$1 Million Identity Fraud Loss Reimbursement Fraud Consultation, and Identity Theft Restoration.

How to Activate Your Services

Visit krollbreach.idMonitoringService.com to activate and take advantage of your identity monitoring services.

*You have until **May 14, 2020** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

If you have questions, please call 1-844-904-0941, Monday through Friday from 8 a.m. to 5:30 p.m. Central Time.

Take Advantage of Your Services

You've been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.