

EXHIBIT 1

The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Texas Orthopaedic & Sports Medicine (“TOSM”) does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On November 28, 2022, TOSM became aware of suspicious activity relating to its internal information systems. In response, TOSM engaged outside forensics and data security specialists to investigate the nature and scope of the activity. TOSM’s investigation has determined that an unauthorized third party gained access to its systems between the dates of November 22, 2022 and November 29, 2022 and took certain information from its systems. In response, TOSM undertook a thorough and comprehensive review of the types of information taken from its systems and potentially subject to access. On February 10, 2023, TOSM determined the information that could have been subject to unauthorized access includes name, driver’s license number, and medical information of one (1) Maine resident.

Notice to Maine Resident

On February 23, 2023, TOSM began providing written notice of this incident to one (1) Maine resident. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, TOSM moved quickly to investigate and respond to the incident, assess the security of TOSM systems, and identify potentially affected individuals. Further, TOSM notified federal law enforcement regarding the event. TOSM is also working to implement additional safeguards and training to its employees. TOSM is providing access to credit monitoring services for one (1) year through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, TOSM is providing impacted individuals with guidance on how to better protect against identity theft and fraud. TOSM is providing individuals with 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 encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

TOSM is providing written notice of this incident to relevant state federal regulators, as necessary. TOSM is also notifying the U.S. Department of Health and Human Services.

EXHIBIT A



February 23, 2023

Dear _____ :

Texas Orthopaedic & Sports Medicine, LLP (“TOSM”) is writing to notify you of a recent incident that may have impacted the security of your personal information. We want to provide you with information about the incident, our response, and steps you may take to better protect against possible misuse of your personal information, should you feel it necessary to do so.

What Happened? On November 28, 2022, we became aware of suspicious activity relating to our internal information systems. In response, we engaged outside forensics and data security specialists to investigate the nature and scope of the activity. Our investigation determined that an unauthorized third party gained access to our systems between the dates of November 22, 2022 and November 29, 2022 and took certain information from our systems. In response, we undertook a thorough and comprehensive review of the types of information taken from our systems and potentially subject to access. On February 10, 2023, we determined that information related to you was impacted during the event.

What Information was Involved? Our investigation determined that your name, date of birth, diagnosis information, disability information, driver's license number, health insurance group/plan number, health insurance information, health insurance policy number, medical history information, medical record number, prescription information, subscriber number, and treating/referring physician, were stored within the impacted systems and therefore potentially accessible by the unauthorized third party. At this time, TOSM is unaware of any actual or attempted misuse of your personal information.

What We Are Doing. The confidentiality, privacy, and security of personal information within our care is among our highest priorities. Upon learning of the event, we investigated to determine the nature and scope of the incident and secured the environment by changing all system passwords. We are also notifying all applicable regulators, including the Department of Health and Human Services. We will be taking additional steps to improve security and better protect against similar incidents in the future.

As an added precaution, TOSM is providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twelve 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. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits forms. Additional information may be found in the attached *Steps You Can Take to Protect Your Information*.

For More Information. We understand you may have questions that are not answered in this letter. If you have questions or concern regarding this incident, we ask that you please contact our dedicated assistance line at 1-833-570-2605 between the hours of 8:00am and 8:00pm Eastern. You may also write to TOSM at 13603 Michel Road Tomball, TX 77375.

Sincerely,

Dr. Tarek Al-Fahl

Dr. Tarek Al-Fahl
Managing Partner
Texas Orthopaedic & Sports Medicine, LLP

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

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

. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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 and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 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 bureaus 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 violator. 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 New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 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. There are 0 Rhode Island residents impacted by this incident.