

# **EXHIBIT 1**

This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, SOA 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 or about July 8, 2021, SOA became aware of suspicious activity relating to an employee email account. SOA immediately launched an investigation to determine what may have happened. Working together with an outside computer forensics specialist, SOA determined that an unauthorized individual accessed several employee email accounts between June 24, 2021 and July 8, 2021. Because SOA was unable to determine which email messages in the accounts may have been viewed by the unauthorized actor, SOA reviewed the entire contents of the affected email accounts to identify what personal information was accessible to the unauthorized actor. This review was complete by October 21, 2021. After identifying the individuals who may have been impacted, SOA worked to confirm current mailing addresses for the impacted individuals and prepare an accurate written notice of this incident.

The information that could have been subject to unauthorized access includes name, and Social Security Number.

### **Notice to Maine Resident**

On or about December 20, 2021, SOA provided written notice of this incident to all affected individuals, which includes approximately 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, SOA moved quickly to investigate and respond to the incident, assess the security of its systems, and notify potentially affected individuals. SOA is also working to implement additional safeguards and training to its employees. SOA is providing access to credit monitoring services for 1 year, through Experian, to individuals whose Social Security numbers were impacted by this incident, at no cost to these individuals.

Additionally, SOA is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. SOA is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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.

# **EXHIBIT A**



Return Mail Processing  
PO Box 589  
Claysburg, PA 16625-0589

December 20, 2021

H1938-L01-0000001 T00001 P001 \*\*\*\*\*SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01 INDIVIDUAL CM  
APT ABC  
123 ANY STREET  
ANYTOWN, ST 12345-6789



**NOTICE OF [Extra1]**

Dear Sample A. Sample:

Southern Orthopaedic Associates d/b/a Orthopaedic Institute of Western Kentucky (“SOA”) is writing to notify you of an incident that may affect the security of some of your personal information. While we are unaware of any actual or attempted misuse of your information, we take this incident very seriously. This letter provides details of the incident and the resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

**What Happened?** On or about July 7, 2021, SOA became aware of suspicious activity relating to an employee email account. We immediately launched an investigation to determine what may have happened. Working together with an outside computer forensics specialist, we determined that an unauthorized individual accessed several employee email accounts between June 24, 2021 and July 8, 2021. Because we were unable to determine which email messages in the accounts may have been viewed by the unauthorized actor, we reviewed the entire contents of the affected email accounts to identify what personal information was accessible. This review was complete by October 21, 2021. Once we identified the individuals who may have been impacted, SOA worked to confirm current mailing addresses for the impacted individuals and prepare an accurate written notice of this incident.

**What Information Was Involved?** Although we cannot confirm whether your personal information was actually accessed, viewed, or acquired without permission, we are providing you this notification out of an abundance of caution, because such activity cannot be ruled out. The following types of your information were located in an email or attachment that may have been accessed or acquired by an unauthorized actor: your name and [Extra2].

**What We Are Doing.** Upon learning of this incident, we changed all employee email account passwords and took steps to secure the impacted accounts. We are currently implementing additional technical safeguards as well as training and education for employees to prevent similar future incidents.

**What You Can Do.** Although we are unaware of any fraudulent misuse of your information, we have arranged to have Experian provide complimentary credit monitoring to you for [Extra3] months as an added precaution. Please review the instructions contained in the enclosed “Steps You Can Take to Protect Your Information” to enroll in and receive these services. SOA will cover the cost of this service; however, you will need to enroll yourself in the credit monitoring service.

0000001



**For More Information.** We recognize that you may have questions not addressed in this letter. If you have additional questions, please contact our dedicated assistance line at (855) 414-6050, Monday through Friday, 8 am – 10 pm Central, or Saturday and Sunday, 10 am – 7 pm Central (excluding major U.S. holidays). You may also write to us at 200 Clint Hill Boulevard, Paducah, KY 42001.

Sincerely,

James Locke  
Chief Executive Officer  
The Orthopaedic Institute of Western Kentucky

## STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

### Enroll in Credit Monitoring

To help protect your identity, we are offering complimentary access to Experian IdentityWorks<sup>SM</sup> for [Extra3] months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for [Extra3] months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration).

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [Extra3]-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by March 31, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [www.experianidworks.com/credit](http://www.experianidworks.com/credit)
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(855) 414-6050** by **March 31, 2022**. Be prepared to provide engagement number **ENGAGE#** as proof of eligibility for the Identity Restoration services by Experian.

### **ADDITIONAL DETAILS REGARDING YOUR [Extra3] MONTHS EXPERIAN IDENTITYWORKS MEMBERSHIP**

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.\*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE<sup>TM</sup>:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance<sup>\*\*</sup>:** Provides coverage for certain costs and unauthorized electronic fund transfers.

\* Offline members will be eligible to call for additional reports quarterly after enrolling.

\*\* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

0000001



## **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](http://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:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
888-298-0045	1-888-397-3742	833-395-6938
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](http://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](mailto: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](http://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](http://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](http://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](http://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 is 1 Rhode Island resident impacted by this incident.

