



LEWIS BRISBOIS BISGAARD & SMITH LLP

Lauren D. Godfrey  
429 Fourth Avenue, Suite 805  
Pittsburgh, Pennsylvania 15219  
Lauren.Godfrey@lewisbrisbois.com  
Direct: 412.567.5113

November 15, 2021

File No. 50130.509

**VIA WEB PORTAL**

Attorney General Aaron Frey  
Office of the Attorney General  
Consumer Protection Division  
Security Breach Notification  
111 Sewall Street, 6th Floor  
Augusta, ME 04330

**Re: Notification of Data Security Incident**

Dear Attorney General Frey:

Lewis Brisbois Bisgaard & Smith LLP represents Lakeshore Bone and Joint Institute, PC (LBJI) in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maine's data breach notification statute.

**1. Nature of the Security Incident**

LBJI is an orthopedic practice located in Indiana.

On July 7, 2021, LBJI discovered unusual activity within its Microsoft Office 365 environment. Immediately upon discovery, LBJI took steps to secure its email environment. Additionally, LBJI retained cybersecurity and digital forensics experts as well as incident response counsel to assist with its response efforts and conduct an investigation to determine the source and scope of the incident.

The investigation revealed that an unauthorized actor was able to access one LBJI e-mail account. Further, the investigation determined personal information may have been impacted as a result of the incident. LBJI then worked diligently to identify address information associated with such individuals in order to provide notification of this incident. This process was completed on October 21, 2021.

## 2. Type of Information and Number of Maine Residents Involved

The incident involved personal information for approximately 1 Maine resident. The information involved differs depending on the individual, but may include Date of Birth, Treatment Information/Diagnosis, Provider Name, MRN/ Patient ID, Health Insurance Information, and Treatment Cost Information.

The affected individual will receive a letter notifying them of the incident and providing additional steps they can take to protect their personal information. For individuals whose Social Security numbers were potentially impacted, LBJI will be offering complimentary identity monitoring services. The notification letters will be sent via USPS First Class Mail on November 15, 2021.

## 3. Measures Taken to Address the Incident

In response to the incident, LBJI retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise.

Additionally, as discussed above, LBJI is notifying the affected individuals and providing them with steps they can take to protect their personal information.

## 4. Contact Information

LBJI is dedicated to protecting the sensitive information within its control. If you have any questions or need additional information regarding this incident, please do not hesitate to contact Lauren Godfrey at [Lauren.Godfrey@lewisbrisbois.com](mailto:Lauren.Godfrey@lewisbrisbois.com).

Sincerely,

*Lauren D. Godfrey*

Lauren D. Godfrey of  
LEWIS BRISBOIS BISGAARD &  
SMITH LLP

LDG:vhn  
Encl.: Sample Notification Letter



Return Mail Processing Center  
P.O. Box 6336  
Portland, OR 97228-6336

To Enroll, Please Call:  
**1-855-288-5422**  
Or Visit:  
**www.MyTrueIdentity.com**  
Activation Code:  
<<Activation Code>>  
Telephone Pass code:  
<<Engagement Number>>

<<Mail ID>>  
<<Name 1>>  
<<Name 2>>  
<<Address 1>>  
<<Address 2>>  
<<Address 3>>  
<<Address 4>>  
<<Address 5>>  
<<City>><<State>><<Zip>>  
<<Country>>

<<Date>>

Re: Notice of Data Security Incident

Dear <<Name 1>>,

I am writing to inform you of a recent data security incident experienced by Lakeshore Bone and Joint Institute, PC (“LBJI”) that may have involved your personal information. At LBJI, we take the privacy and security of all of the information in our possession very seriously. That is why we are writing to notify you of the incident and to provide you with steps that you can take to help protect your personal information.

**What Happened.** On July 7, 2021, LBJI discovered unusual activity within our Microsoft Office 365 environment. Upon discovery, we took immediate steps to secure the email environment. In addition, we retained outside cybersecurity experts to conduct an investigation to determine the source and scope of the incident.

The investigation revealed that an unauthorized actor was able to access an LBJI employee’s e-mail account. Based on the findings from the investigation, we reviewed the affected account to determine what data might have been impacted. We determined that the impacted account contained some of your personal information. We then worked diligently to identify addresses for the individuals whose information may have been involved which was completed on October 21, 2021. Importantly, LBJI is not aware of any misuse of your personal information as a result of this incident.

**What Information Was Involved.** The information may have involved your name, <<Breached Elements>>.

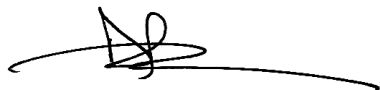
**What We Are Doing.** As soon as we detected the incident, we took the measures referenced above. We are also providing you with information about steps you can take to help protect your personal information, and offering free credit monitoring services for <<CM Length>> through TransUnion as described below.

**What You Can Do.** You can follow the recommendations included with this letter to protect your personal information. We also strongly encourage you to enroll in the credit monitoring and identity monitoring services we are offering through TransUnion. To enroll in this service, go to [www.MyTrueIdentity.com](http://www.MyTrueIdentity.com) or call **1-855-288-5422** and when prompted for the Activation Code, provide << Activation Code>> and follow the steps to receive your credit monitoring services. Your complimentary services will include credit monitoring, fraud alerts, and \$1,000,000 in identity theft insurance. The deadline to enroll is <<Enrollment Deadline>>.

**For More Information:** If you have any questions regarding the incident or would like assistance with enrolling in the credit and identity monitoring services, please call 855-675-3108 between 9am to 9pm Eastern Time from Monday to Friday.

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 be 'Dale Ingram', with a long horizontal flourish extending to the right.

Dale Ingram  
Chief Executive Officer  
Lakeshore Bone and Joint Institute, PC

## 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](http://www.equifax.com)

**Experian**  
P.O. Box 9532  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

**TransUnion**  
P.O. Box 1000  
Chester, PA 19016  
1-800-916-8800  
[www.transunion.com](http://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](http://consumer.ftc.gov), and  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)  
1-877-438-4338

**Maryland Attorney General**  
200 St. Paul Place  
Baltimore, MD 21202  
[oag.state.md.us](http://oag.state.md.us)  
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](http://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](http://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://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.



Return Mail Processing Center  
P.O. Box 6336  
Portland, OR 97228-6336

<<Mail ID>>  
<<Name 1>>  
<<Name 2>>  
<<Address 1>>  
<<Address 2>>  
<<Address 3>>  
<<Address 4>> <<Date>>  
<<Address 5>>  
<<City>><<State>><<Zip>>  
<<Country>>

Dear <<Name 1>>,

I am writing to inform you of a recent data security incident experienced by Lakeshore Bone and Joint Institute, PC (“LBJI”) that may have involved your personal information. At LBJI, we take the privacy and security of all of the information in our possession very seriously. That is why we are writing to notify you of the incident and to provide you with steps that you can take to help protect your personal information.

**What Happened.** On July 7, 2021, LBJI discovered unusual activity within our Microsoft Office 365 environment. Upon discovery, we took immediate steps to secure the email environment. In addition, we retained outside cybersecurity experts to conduct an investigation to determine the source and scope of the incident.

The investigation revealed that an unauthorized actor was able to access an LBJI employee’s e-mail account. Based on the findings from the investigation, we reviewed the affected account to determine what data might have been impacted. We determined that the impacted account contained some of your personal information. We then worked diligently to identify addresses for the individuals whose information may have been involved which was completed on October 21, 2021. Importantly, LBJI is not aware of any misuse of your personal information as a result of this incident.

**What Information Was Involved.** The information may have involved your name, <<Breached Elements>>.

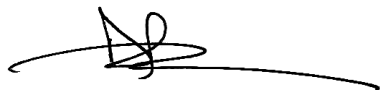
**What We Are Doing.** As soon as we detected the incident, we took the measures referenced above. We have also taken steps to help prevent a similar incident from occurring in the future. LBJI is also providing notice of this incident to potentially impacted individuals and providing steps one can take to help protect their information. LBJI has also established a toll-free call center to answer questions about the incident. Call center representatives are available Monday through Friday from 9 am – 9 pm Eastern Time and can be reached at 855-675-3108.

**What You Can Do.** LBJI encourages individuals to remain vigilant against incidents of identity theft and fraud, to review account statements and explanations of benefits forms, and to monitor free credit reports for suspicious activity and to detect errors. The recommendations included with this letter includes more steps you can take to protect your personal information.

**For More Information:** If you have any questions regarding the incident please call 855-675-3108 between 9am to 9pm Eastern Time from Monday to Friday.

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 be 'Dale Ingram', with a long horizontal flourish extending to the right.

Dale Ingram  
Chief Executive Officer  
Lakeshore Bone and Joint Institute, PC

## 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](http://www.equifax.com)

**Experian**  
P.O. Box 9532  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

**TransUnion**  
P.O. Box 1000  
Chester, PA 19016  
1-800-916-8800  
[www.transunion.com](http://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](http://consumer.ftc.gov), and  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)  
1-877-438-4338

**Maryland Attorney General**  
200 St. Paul Place  
Baltimore, MD 21202  
[oag.state.md.us](http://oag.state.md.us)  
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](http://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](http://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://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.