

G E O R G I A
BONE & JOINT
 SURGEONS, P.C.
 P.O Box 989728
 West Sacramento, CA 95798-9728

To enroll, Please Call:
 1-833-806-0314
 Or Visit:
<https://app.idx.us/account-creation/protect>
 Enrollment Code: <<Enrollment>>

<<First Name>> <<Last Name>>
 <<Address1>>
 <<Address2>>
 <<City>>, <<State>> <<Zip>>

February 25, 2022

NOTICE OF <<Variable Heading>>

Dear <<First Name>> <<Last Name>>:

Georgia Bone & Joint Surgeons, P.C. (“Georgia Bone”) is writing to notify you of an 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 is necessary to do so.

What Happened? On or about October 20, 2021, Georgia Bone became aware of a malware incident impacting certain company systems. We immediately worked to restore our systems and launched an investigation, with assistance from third-party computer forensic specialists, to determine the nature and scope of the incident. Through the investigation, Georgia Bone determined that certain information may have been subject to unauthorized access and/or acquisition during the incident from October 15, 2021 to October 20, 2021. Therefore, we reviewed our files and conducted a comprehensive programmatic and manual review of the potentially impacted information to determine the type of information and to whom it related. On January 18, 2022, we completed this review and obtained contact information to notify potentially impacted individuals about this event. We also worked to engage additional services and resources for these individuals. Although we are unaware of any actual or attempted misuse of your personal information, we are providing you this notice out of an abundance of caution.

What Information Was Involved? Although the investigation is ongoing, it was determined that the involved Georgia Bone systems may have contained the following types of your information at the time of the incident: name, address, <<Data Element>>. To date, we have no evidence that any of your information has been misused.

What We Are Doing. We take this incident and the security of personal information in our care very seriously. Upon learning of this incident, we moved quickly to investigate and respond to this incident, assess the security of our systems, restore functionality to our environment, and notify potentially affected individuals. As part of our ongoing commitment to the security of information, we notified federal law enforcement and are reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event. As a precautionary measure, we are notifying potentially affected individuals, including you, so that you may take further steps to best protect your personal information, should you feel it is appropriate to do so. We regret any inconvenience or concern this incident may cause. As an added precaution, Georgia Bone is offering you access to <<12/24>> months of free credit monitoring and identity protection services through IDX at no cost to you.

What You Can Do. Please review the enclosed *Steps You Can Take to Protect Personal Information*, which contains information on what you can do to better protect against possible misuse of your information. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, explanation of benefits,

and credit reports. Any suspicious activity should be reported to your provider or financial institution as soon as possible. You will also find information on how to enroll in the credit monitoring and identity protection services being offered.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call the dedicated assistance line at 1-833-806-0314, 9 am to 9 pm ET. Individuals may also write to Georgia Bone at: 15 Medical Drive NE Cartersville, GA 30121.

We take the privacy and security of personal information in our care seriously, and sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "A. Riddle".

Andrew Riddle, M.D.

Orthopedic Surgeon

Georgia Bone & Joint Surgeons, P.C.

Steps You Can Take to Protect Personal Information

Enroll in Credit Monitoring and Identity Protection Services

- 1. Website and Enrollment.** Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
- 2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
- 3. Telephone.** Contact IDX at 1-833-806-0314 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit 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	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; 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.