Greater Pittsburgh Orthopedic Associates Inc.
c/o Cyberscout
<<Return Address>>
<<City>>, <<State>> <<Zip>>

<<FirstName>> <<LastName>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<PostalCode+4>>

<<Date>>

Via First-Class Mail

<<Custom Field 1>>

Dear <<FirstName>> <<LastName>>,

Greater Pittsburgh Orthopedic Associates Inc. ("GPOA") experienced a data security incident that may have affected your personal information. We have no indication that your information has been or will be misused. We want to make you aware of the incident and the measures we have taken in response, as well as provide details on steps you can take – should you deem it appropriate – to help protect your information. The protection, privacy, and proper use of your information is paramount, and we are working to prevent this type of incident from occurring again.

What Happened

GPOA detected an incident on August 10, 2025, involving unauthorized access to GPOA's computer network. We immediately initiated our incident response, engaged additional third-party experts, and commenced an investigation. These specialized third parties secured our environment, hardened and enhanced our network security, and have completed a digital forensic investigation to determine the extent of unauthorized activity within GPOA's network. Unfortunately, these types of incidents have become increasingly common and even organizations with the most sophisticated IT infrastructure available are affected. We have worked diligently to determine what happened and what information could have been compromised.

What Information Was Involved

With the assistance of the third-party digital forensic investigation, we determined that your personal information could have been compromised. While the impacted data elements vary, this compromise could have included your name, mailing address, Social Security number, and provider name. Please note that we have no evidence at this time that any of your personal information has been misused as a result of the incident.

What We Are Doing

We take this incident seriously and are committed to the strength of our systems' security to prevent a similar event from occurring in the future. We are also focused on continuous awareness training and assessment of our data security. We have notified law enforcement regarding this incident.

Additionally, out of an abundance of caution, we have arranged for you to activate Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge for 24 months

through Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. To enroll in these services, please follow the instructions provided within ninety (90) days from the date of this letter. You can enroll by using enrollment code <<**UniqueCode**>> and visiting *https://bfs.cyberscout.com/activate*.

Please note that to activate monitoring services, you will need an internet connection and e-mail account. Additionally, you may be required to provide your name, date of birth, and Social Security number to confirm your identity. Due to privacy laws, we cannot register you directly. Certain services might not be available for individuals who do not have a credit file with the credit bureaus or an address in the United States (or its territories) and a valid Social Security number. Activating this service will not affect your credit score.

What You Can Do

We are not aware of anyone experiencing fraud as a result of this incident. As data incidents are increasingly common, we encourage you to always remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information. We encourage you to review the Additional Important Information located on the following pages, which includes further steps to safeguard your personal information, such as implementing a fraud alert or security freeze.

For More Information

If you have any questions, call 833-866-3587 between 6:00 AM and 6:00 PM PT, Monday through Friday, excluding holidays. Please know that GPOA values the protection of our network and the privacy of your personal information, and we understand the concern that these incidents cause.

Sincerely,

Greater Pittsburgh Orthopedic Associates Inc.
5820 Centre Ave.
Pittsburgh, PA 15206

Additional Important Information

Monitoring: You should always remain vigilant and monitor your accounts for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for suspicious or unusual activity. You can report suspicious activity to financial institutions or law enforcement.

Fraud Alert: You can place fraud alerts with the three major credit bureaus by phone and online as set forth below with Equifax, TransUnion, or Experian. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can get an extended fraud alert for seven years.

Credit Report: Consumers are also entitled to one free credit report annually from each of the three credit reporting bureaus. To order your free credit report: visit *www.annualcreditreport.com*; call, toll-free, 1-877-322-8228; or mail a completed Annual Credit Report Request Form (available at *https://www.consumer.ftc.gov/articles/0155-free-credit-reports*) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information may need to be included when requesting a security freeze: (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current and addresses for the past five years; (5) proof of address; (6) Social Security Card, pay stub, or W2; or (7) government-issued identification card. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

TransUnion	**Experian**	**Equifax**
1-888-909-8872	1-888-397-3742	1-800-349-9960
www.transunion.com/credit-help	*www.experian.com/help/*	*www.equifax.com/personal/credit-report-services/*
Fraud Alert P.O. Box 2000 Chester, PA 19016	Fraud Alert P.O. Box 9554 Allen, TX 75013	Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069
Credit Freeze P.O. Box 160, Woodlyn, PA 19094	Credit Freeze P.O. Box 9554, Allen, TX 75013	Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788

Implementing an Identity Protection PIN (IP PIN) with the IRS: To help protect against a fraudulent tax return being filed under your name, we recommend Implementing an Identity Protection PIN (IP PIN) with the IRS. An IP PIN is a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS. It helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account.

If you don't already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft. The fastest way to receive an IP PIN is by using the online Get an IP PIN tool found at: *https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin*. If you wish to get an IP PIN and you don't already have an account on IRS.gov, you must register and validate your identity.

Spouses and dependents are eligible for an IP PIN if they can pass the identity verification process. Some items to consider when obtaining an IP PIN with the IRS: (1) an IP PIN is valid for one calendar year; (2) a new IP PIN is generated each year for your account; (3) logging back into the Get an IP PIN tool, will display your current IP PIN; and (4) an IP PIN must be used when filing any federal tax returns during the year including prior year returns.

Fair Credit Reporting Act: Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting *https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf*, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Federal Trade Commission: More information can be obtained by contacting the Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) *www.ftc.gov/idtheft*.

***For Massachusetts residents*:** You can obtain a police report if you are a victim of identity theft.

***For Iowa residents*:** You can report any suspected identity theft to law enforcement or to the Attorney General.

***For Oregon residents*:** You can report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

***For Vermont residents*:** If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

Residents of the below states can obtain additional information regarding identify theft and more at:

- ***District of Columbia Attorney General***: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and *https://oag.dc.gov*.
- ***Maryland Office of the Attorney General***: Consumer Protection Division, 200 St. Paul Place, 16th Fl, Baltimore, MD 21202; 1-888-743-0023; *https://www.marylandattorneygeneral.gov*.
- ***New York Attorney General***: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or *https://ag.ny.gov*.
- ***North Carolina Attorney General***: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and *https://www.ncdoj.gov*.