BAKER DONELSON
BEARMAN, CALDWELL & BERKOWITZ, PC

ONE EASTOVER CENTER
100 VISION DRIVE, SUITE 400
JACKSON, MISSISSIPPI 39211

P.O. BOX 14167
JACKSON, MISSISSIPPI 39236

PHONE: 601.351.2400
FAX: 601.351.2424

www.bakerdonelson.com

BRAD C. MOODY
Direct Dial: 601.351.2420
Direct Fax: 601.592.2420
E-Mail Address: bmoody@bakerdonelson.com

July 5, 2018

Attorney General Gordon MacDonald
Attn: Consumer Protection and Antitrust Bureau
33 Capitol Street
Concord, NH 03301
doj-cpb@doj.nh.gov

Re: *MSK Group, P.C.*

Dear Attorney General MacDonald:

I serve as outside legal counsel to MSK Group, P.C. ("MSK"), a physician practice group that is headquartered at 6077 Primacy Pkwy, Suite 140 Memphis, Tennessee 38119. MSK has offices in Memphis, Tennessee; Marion, Arkansas; and Southaven, Mississippi, and primarily serves patients in the States of Tennessee, Arkansas, and Mississippi.

This correspondence is to notify you[1] of a recent security event. **PLEASE NOTE:** MSK does ***not*** believe any personally identifiable personal information ("PII") was actually acquired (i.e. PII was not removed) from MSK's computer network.

However, in an abundance of caution, notification letters are being sent to 8 residents of NH on July 5, 2018. Sample notification letters are enclosed for your reference and include -

- A description of the security event;
- Steps taken to investigate;
- Steps taken to mitigate any potential harm to consumers;
- Steps taken to prevent this type of security event in the future,

[1] MSK does not waive (and reserves the right to assert) any and all defenses related to this matter. MSK also does not waive any jurisdictional defenses by voluntarily submitting this notice. This notice should not be construed in any way as an attempt by MSK to avail itself of the laws of this State.

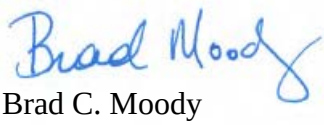
- Instructions for activation of 1-year of free Identity Theft Protection services that include credit monitoring and a $1 million insurance reimbursement policy to all consumers who received notification; and
- Instructions regarding how to obtain more information about this event; etc.

MSK is a HIPAA covered entity, and as such, is also notifying The United States Department of Health & Human Services, Office for Civil Rights pursuant to the HIPAA - HITECH Breach Notification Regulations.

MSK is fully committed to protecting consumer privacy and the confidentiality of personal information. We will follow-up this correspondence with any forms or other documents that may need to be completed. Please contact me if you require any additional information regarding this incident.

Best regards,

BAKER, DONELSON, BEARMAN,
CALDWELL & BERKOWITZ, PC



Brad C. Moody

Enclosure:

Exhibit 1: Sample Notification Letter sent to 8 residents

MSK Group, PC
C/O ID Experts
P.O. Box 10444
Dublin, Ohio 43017-4044

To Enroll in ID Protection, Please Visit:

https://ide.myidcare.com/mskprotect

Enrollment Code: [XXXXXXXX]

<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

July 5, 2018

Dear <<FirstName>> <<LastName>>:

MSK Group, PC[1] sincerely appreciates that you have entrusted us with your orthopedic care and the confidentiality of your information. As such, we want to notify you of a data security event.

What Happened? On May 7, 2018, we discovered that our computer networks were subject to a security event. We hired expert consultants to investigate, mitigate, and assess the extent of this event and to help further strengthen our information security.

NOTE: As of today, we do not believe that any part of your medical record was actually removed from our computer network. However, because there was unauthorized access to our network at times over several months and data was encrypted on approximately May 7, we felt it most prudent to notify you and to offer you **free Identity Theft Protection** and additional information regarding how you can protect yourself from any potential harm.

What Information Was Involved? Your full name, address, date of birth, age, date of service, medical record number, phone number, email address, social security number, health insurance information, facsimile number, driver's license, medical device number, facial photos, diagnostic images, and other information commonly found in a medical record, were potentially affected. **Fortunately, we do NOT believe any bank account or credit card numbers were affected, and we do not believe that any part of your medical record was actually removed from our computer network.**

What We Are Doing? We extensively investigated this matter, and reported this to the FBI. We are taking steps to further secure patient information. We are also offering you 1-year of **free Identity Theft Protection services that include credit monitoring and a $1 million insurance reimbursement policy. For instructions on how to activate these services, please see below**.

What You Can Do? Activate your FREE Identity Theft Protection.[2] We are offering free identity theft protection services through ID Experts® to provide you with MyIDCare™. MyIDCare services include: 12 months of credit monitoring, a $1 million insurance reimbursement policy with no deductible from an A.M. Best "A-rated" carrier, and fully managed ID theft recovery services. With this protection, MyIDCare will help you resolve issues, if your identity is ever compromised.

- **Enroll in free MyIDCare services by going to https://ide.myidcare.com/mskprotect and using the Enrollment Code provided above. Please note: The deadline to enroll is 90 days from the date of this letter.**

For more information about this incident, please call toll-free **1-888-675-4771 Monday through Friday 7 am to 7 pm CT**. We are fully committed to protecting the confidentiality of your information and sincerely apologize for any inconvenience this situation has caused you. Thank you for allowing us to serve as your orthopedic healthcare provider.

Sincerely,

Kimble L. Jenkins, CEO

[1] MSK Divisions are OrthoMemphis, Memphis Orthopaedic Group, Tabor Orthopedics, and Crosstown Back & Pain Institute.
[2] Minors under age 18 typically do not have established credit history and are under the age to secure credit, so credit monitoring may not be applicable. All other services still apply. Minors should take all the additional steps noted in this letter.

Exhibit 1

ADDITIONAL STEPS YOU MAY WANT TO TAKE

- **ORDER YOUR FREE ANNUAL CREDIT REPORTS.** Visit www.annualcreditreport.com or call 877-322-8228 to obtain 1 free copy of your credit report annually. Periodically review a copy of your credit report for discrepancies, and report any accounts you did not open or inquiries you did not authorize.
- **REVIEW ACCOUNT STATEMENTS.** Remain vigilant and periodically review your credit reports, bank/credit card, insurance and account statements. Create alerts on credit/bank accounts to notify of suspicious activity.
- **REPORT** suspicious or fraudulent charges to your insurance statements, credit report, credit card or bank accounts to your insurance company, bank/credit card vendor and law enforcement. (For Oregon & Iowa residents: Report any suspected identity theft to law enforcement, Federal Trade Commission, and your State Attorney General.)
- **PLACE FRAUD ALERTS ON YOUR CREDIT FILE.** A fraud alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. After placing a fraud alert, a lender should verify that you have authorized the request before allowing any actions regarding your credit. Contact one of the credit reporting agencies to activate a fraud alert:

3 MAJOR CREDIT BUREAUS / CONSUMER REPORTING AGENCIES

Equifax	Experian	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

- **POLICE REPORT:** You have a right to a police report about this incident (if any exists). If you're an identity theft victim, you have the right to file a police report and obtain a copy of it.
- **CONTACT FTC OR STATE ATTORNEY GENERAL'S OFFICE FOR MORE INFORMATION ON HOW TO AVOID IDENTITY THEFT.** For Maryland residents: MD State Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023. For North Carolina Residents: NC Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226. For Rhode Island Residents: 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400.Federal Trade Commission (600 Pennsylvania Ave., NW, Washington, DC 20580) also provides information about identity theft protection at www.ftc.gov/idtheft & 877-438-4338.
- **PLACE A SECURITY FREEZE ON YOUR CREDIT FILE.** Placing a freeze on your credit report will prevent lenders, etc. from accessing your credit report and the extending of credit in connection with a new credit application. S ecurity freeze may not apply to existing accounts and when a copy of your report is requested by your existing creditor for certain types of account review, collection, fraud control or similar activities. To place a security freeze on your credit report, send a written request to each of the 3 major consumer reporting agencies: (Equifax, Experian, and TransUnion - addresses are above). To request a security freeze, provide the following information: full name (including middle initial, Jr., Sr., II, III, etc.), social security number; Date of birth; If you have moved in the past 5 years, provide addresses where you have lived over prior 5 years; Proof of current address such as a current utility /telephone bill; A legible photocopy of a government issued identification card (state driver's license or ID card, military ID, etc.); If you are a victim of identity theft, include a copy of either the police report, investigative report, or law enforcement complaint concerning identity theft; If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail. Credit reporting agencies have 3 business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within 5 business days and provide you a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze. To lift a security freeze to allow a specific entity/individual access to your credit report, call/send a written request to the credit reporting agencies by mail and include proper identification (name, address, social security number) and PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities/individuals you would like to receive your credit report or the specific period of time you want the credit report available. Credit reporting agencies have 3 business days after receiving a request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, send a written request to each of the 3 credit bureaus by mail and include proper identification (name, address, and social security number) and PIN number or password provided to you when you placed the security freeze. Credit bureaus have 3 business days after receiving request to remove the freeze.
  (For MA residents: The fee for each placement of a freeze, temporary lift of a freeze, or removal of a freeze is $5.)