GEORGIA SPINE & ORTHOPAEDICS

SUBSTITUTE NOTICE

Georgia Spine and Orthopaedics of Atlanta ("GSO") was a recent victim of an email "phishing" scam that resulted in unauthorized access to an employee's email account. "Phishing" involves scammers sending emails that look legitimate, but in reality, are fraudulent. The emails often have malicious links or documents within them that, when accessed, allow the scammer to gain the email account/passwords - often without the knowledge of the email account owner. Companies all over the world are faced with the threat of phishing scams every day, as scammers get more and more sophisticated.

Unfortunately, phishing scams are hard to detect. Upon discovery of the incident, we promptly terminated the unauthorized access. We also engaged outside technical and legal experts to investigate the incident thoroughly to determine the full nature and scope of the access, to ensure our information technology systems are truly secure, and to identify (through a very tedious technical assessment and hand document review process) the exact emails that were actually accessed by the third party. After expert analysis, it was determined that the unauthorized access occurred on July 11, 2018. Because of the way the email account was accessed, a desk copy of certain emails was potentially saved onto the computer of the unauthorized third party - likely unintentionally, but we had to assume that the third party retained a copy of that data. As such, we searched the emails to determine whether sensitive data was located within any of the emails that were potentially saved. Individual emails were then hand reviewed to obtain names and mailing addresses.

After completing this extensive review, on October 26, 2018, we were alerted by the reviewers' final mailing list that the mailbox included patient names and other information typically found in a medical record. A smaller number of the emails contained Social Security numbers and/or driver's license numbers.

Fortunately, the unauthorized access did not extend beyond the single email account. We have attempted to notify by letter those for whom we had mailing addresses. GSO has advised affected persons to remain vigilant and monitor account statements and credit reports carefully and to report discrepancies to law enforcement. Fraud alerts and security freezes also can be activated to help protect individuals.

GSO has set up a toll free hotline to address any questions or concerns. If you are concerned your information was included in this incident, please call 888-238-5166, Monday through Friday, from 9 am to 9 pm EST for the next 90 days.

###