April 15, 2019

Notice of Recent Email Phishing Incident

National Seating & Mobility, Inc.("NSM") is hereby notifying individuals of an email phishing incident that resulted in unauthorized access to NSM email boxes on or about February 14, 2019. These email boxes may have contained personal information for some individuals.

Fortunately, the incident was limited to only certain employee email accounts, and did NOT affect NSM's overall medical / billing / human resources records systems. Also, NSM has NOT received any report of identity theft as the result of this incident.

> Phishing involves an outside person sending an email that looks perfectly legitimate, but in reality, the email has a malicious link or document within the email that, when accessed, allows the outside person to gain access to the recipient's email account/passwords – often without the knowledge of the email account owner.

NSM promptly responded to this phishing incident - changing all passwords and utilizing state of the art technology to block suspicious activity and unauthorized access. As of February 14, it appeared that the perpetrator likely would not have had time to access/copy/download individual emails containing personal information.

In an abundance of caution, we reached out to outside technical experts to request assistance in further investigating the incident in order to evaluate the full nature and scope of any potential access to ensure there was no access to individual personal information.

On March 12, we were alerted by these experts that, because of the method of access, some of the email accounts may have been at risk of being copied - likely inadvertently during the standard email synchronization process.

We then conducted an extensive document review process to determine whether individual names or other sensitive data were located within any of the emails that may have been affected.

We are in the process of sending a notification letter to the individuals (for whom we have a mailing address) where we determined that personal information was potentially involved.

To date, it appears the information potentially synced was full name, address, date of birth, diagnoses/diagnostic codes and other information typically used to order a mobility device. In some instances, social security numbers, driver's license numbers, Medicare/Medicaid numbers, health insurance information or the customer's guarantor's personal information may have been in the affected email accounts.

NSM values the safety and security of client and employee information and is continuing to take steps to enhance its security measures to help prevent something like this from happening in the future.

While we have no evidence that any personal information has actually been used inappropriately, we recommend affected persons remain vigilant and monitor financial account statements and credit reports carefully and report discrepancies to law enforcement. Fraud alerts and security freezes also can be activated to help protect individuals. NSM is providing identity theft monitoring to any individual whose social security number was potentially within the email accounts.

NSM is setting up a toll free call center to answer questions, which will be available for 90 days starting on **April 16, 2019**. If you are concerned your information was involved in this incident, please call 866-511-7204 Monday through Friday from 8 a.m. to 5:30 p.m. CST, excluding holidays, to verify and obtain additional information regarding whether your information was potentially affected.