

## AG CONSUMER [AG]

---

**From:** stanleys@gtlaw.com  
**Sent:** Wednesday, September 21, 2016 4:08 PM  
**To:** AG CONSUMER [AG]  
**Cc:** mattiolim@gtlaw.com  
**Subject:** Data Breach/Security Notification  
**Attachments:** 317671737\_1\_lowa - Data Breach Notification.pdf; 317671435\_1\_NJ Spine Center Breach Notification Letter.pdf

Good afternoon,

Please see the attached correspondence sent on behalf of Mark L. Mattioli.

Thank you.

Stephen J. Stanley  
Litigation Paralegal  
Greenberg Traurig, LLP | 2700 Two Commerce Square | 2001 Market Street | Philadelphia, PA 19103  
Main 215.988.7800 | Direct: 215.988.7807 | Fax: 215.717.5203  
[stanleys@gtlaw.com](mailto:stanleys@gtlaw.com) | [www.gtlaw.com](http://www.gtlaw.com)



---

If you are not an intended recipient of confidential and privileged information in this email, please delete it, notify us immediately at [postmaster@gtlaw.com](mailto:postmaster@gtlaw.com), and do not use or disseminate such information.



Mark Mattioli  
Tel 215.988.7884  
mattiolim@gtlaw.com

September 21, 2016

VIA EMAIL

Office of the Attorney General of Iowa  
Consumer Protection Division  
Security Breach Notifications  
1305 E. Walnut Street  
Des Moines, Iowa 50319-0106

Re: Data Breach Notification Pursuant to Iowa Code §§ 715C.1, 715C.2

To Whom It May Concern:

I represent the New Jersey Spine Center ("NJSC"), which is located at 40 Main St. in Chatham, NJ 07928. On July 27, 2016, NJSC was the victim of a ransomware attack (CryptoWall) that encrypted its patient records and disabled its telephone systems. The information would contain date of birth, and in some cases SSN, driver's license and payment information such as credit card and bank information. The hackers demanded a payment be made to them so that the practice could be provided with an encryption key to unlock the files. NJSC paid the ransom to unlock the files and notified the New Jersey office of the FBI and NJ State police. We have no reason to believe that any of the information was retrieved by the hackers for identify theft purposes.

Appropriate notification letters are being sent to all affected patients pursuant to The Health Information Technology for Economic and Clinical Health (HITECH) Act. A sample copy of the letter is enclosed. NJSC will offer complimentary credit monitoring to all its patients (approximately 28,000). The Office of Civil Rights of the Department of Health and Human Services and credit reporting agencies will also be notified of the incident.

With regard to the State of Iowa, one (1) individual was notified of the incident. While NJSC is not licensed in the State of Iowa, and does not do business in the state or solicit patients from the state, we are nevertheless advising you of this incident.

Please give me a call at the above telephone number if you have any questions.

Kind regards,

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

Mark Mattioli  
Shareholder

MM:ss



## New Jersey Spine Center

Return Mail Processing Center  
PO Box 6336  
Portland, OR 97228-6336

<<mail id>>  
<<Name>>  
<<Street Address>>  
<<City, State Zip>>

<<Date>>

Dear Ms./Mr. <<Name>>,

The privacy, security and confidentiality of the information we maintain for our patients is a top priority for everyone at the New Jersey Spine Center. Regrettably, we are writing to inform you we have had a security incident.

On July 27, 2016, our computer systems were attacked by a malware ransom virus called "CryptoWall." The malware was detected by our virus protection software but unfortunately not until after our electronic patient records were encrypted. The virus encrypted, thereby rendering unusable, all of our electronic medical record files that contained all of the clinical information on our patients such as procedures, office notes, reports, etc. In addition to the medical information, the records contained demographic information such as date of birth, address, and in some cases SSN, credit card and account information. The virus also encrypted our most recent system backup and even disabled our phone system. The individuals demanded that we pay a monetary ransom in order to receive an encryption key to unlock the files. Seeing no other option, we elected to pay the ransom to gain access to the records. We notified the FBI and local authorities regarding the incident. Unfortunately, these individuals often operate outside of the United States, making detection, identification and prosecution nearly impossible.

The virus likely utilized a list of stolen passwords and ran an automated program that attempted access until a correct match was found.

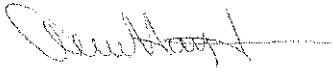
While we cannot guarantee that patient personal demographics were not the target for the intrusion, we have no information that would suggest the attack was an effort to steal patient information. Further, we have no information to suggest that any of your medical or financial information was used or acquired by the hackers for any improper purpose.

In an abundance of caution, we are notifying you of this incident and providing you with the option to obtain complimentary credit monitoring. To further protect yourself, you should be diligent and review your record with your physician at your next appointment to verify your information if anything seems incorrect.

We have partnered with Equifax® to provide its Credit Watch™ Gold identity theft protection product for one year at no charge to you. A description of this product is provided in the attached materials, which also contains instructions about how to enroll (including your personal activation code). If you choose to take advantage of this product, it will provide you with a notification of any changes to your credit information, up to \$25,000 Identity Theft Insurance Coverage and access to your credit report. You must complete the enrollment process by January 15, 2017. We urge you to consider enrolling in this product, at our expense, and review the Additional Resources enclosed with this letter.

If you have additional questions regarding this incident, please call the following toll free number: 844-749-5102.

Sincerely,

A handwritten signature in cursive script, appearing to read "Sharon Hayden", with a horizontal line extending to the right.

Sharon Hayden  
Practice Manager  
New Jersey Spine Center



Activation Code: <<INSERT Credit Monitoring Code>>

<p><u>About the Equifax Credit Watch™ Gold identity theft protection product</u></p> <p>Equifax Credit Watch will provide you with an “early warning system” to changes to your credit file. Note: You must be over age 18 with a credit file in order to take advantage of the product.</p>	<p>Equifax Credit Watch provides you with the following key features and benefits:</p> <ul style="list-style-type: none"><li>○ Comprehensive credit file monitoring and automated alerts of key changes to your <b>Equifax</b> credit report</li><li>○ Wireless alerts and customizable alerts available (available online only)</li><li>○ Access to your Equifax Credit Report™</li><li>○ Up to \$25,000 in identity theft insurance with \$0 deductible, at no additional cost to you †</li><li>○ Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m. to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance, and help initiate an investigation of inaccurate information.</li><li>○ 90 day Fraud Alert placement with automatic renewal functionality* (available online only)</li></ul>
--	---

**How to Enroll: You can sign up online or over the phone**

<p>To sign up online for <b>online delivery</b> go to <a href="http://www.myservices.equifax.com/gold">www.myservices.equifax.com/gold</a></p> <ol style="list-style-type: none"><li>1. <u>Welcome Page</u>: Enter the Activation Code provided at the top of this page in the “Activation Code” box and click the “Submit” button.</li><li>2. <u>Register</u>: Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the “Continue” button.</li><li>3. <u>Create Account</u>: Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the “Continue” button.</li><li>4. <u>Verify ID</u>: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the “Submit Order” button.</li><li>5. <u>Order Confirmation</u>: This page shows you your completed enrollment. Please click the “View My Product” button to access the product features.</li></ol>	<p>To sign up for <b>US Mail delivery</b>, dial 1-866-937-8432 for access to the Equifax Credit Watch automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only.</p> <ol style="list-style-type: none"><li>1. <u>Activation Code</u>: You will be asked to enter your enrollment code as provided at the top of this letter.</li><li>2. <u>Customer Information</u>: You will be asked to enter your home telephone number, home address, name, date of birth and Social Security Number.</li><li>3. <u>Permissible Purpose</u>: You will be asked to provide Equifax with your permission to access your credit file and to monitor your file. Without your agreement, Equifax cannot process your enrollment.</li><li>4. <u>Order Confirmation</u>: Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided). Please allow up to 10 business days to receive this information.</li></ol>
--	---

Directions for placing a Fraud Alert

A fraud alert is a consumer statement added to your credit report. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. To place a fraud alert on your credit file, visit: [https://www.alerts.equifax.com/AutoFraud\\_Online/jsp/fraudAlert.jsp](https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp) or you may contact the Equifax auto fraud line at 1-877-478-7625, and follow the simple prompts. Once the fraud alert has been placed with Equifax, a notification will be sent to the other two credit reporting agencies, Experian and Trans Union, on your behalf.

† Identity Theft Insurance underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions. This product is not intended for minors (under 18 years of age).

\* The Automatic Fraud Alert feature made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.