

# FREEMAN MATHIS & GARY

A LIMITED LIABILITY PARTNERSHIP

100 Galleria Parkway  
Suite 1600  
Atlanta, Ga. 30339-5948

Tel: 770.818.0000  
Fax: 770.937.9960

www.fmglaw.com

David A. Cole  
Partner

Writer's Direct Access  
770.818.1287

dcole@fmglaw.com

July 6, 2017

RECEIVED

JUL 10 2017

CONSUMER PROTECTION

## VIA U.S. MAIL

Attorney General Joseph Foster  
Office of the Attorney General  
New Hampshire Department of Justice  
33 Capitol Street  
Concord, NH 03301

### **Re: Notice of Breach in the Security of Personal Information**

To Whom It May Concern:

I represent Peachtree Neurological Clinic ("PNC"), which is a neurological services provider located in Atlanta, Georgia. This letter is being provided pursuant to N.H. Rev. Stat. § 359-C:20, which requires that your office be notified in the event of a breach in the security of personal information affecting residents of the state of New Hampshire.

Recently, PNC's computer system was infected by a ransomware virus that encrypted its electronic medical records system containing its patients' medical records. The ransomware demanded monetary payment from PNC in order to decrypt the files and allow the practice to regain access to them. PNC did not pay the ransom to the cyber criminals, but were instead able to restore its files and the functionality of its system through backup records. The encryption did not substantially impair PNC's ability to provide care to its patients. Subsequent scans of PNC's system show no further sign of the ransomware, and its investigation does not show any indication that the ransomware exfiltrated any data off its system.

However, through its investigation of the incident, PNC discovered on May 10, 2017, that its computer system previously had been accessed without its knowledge by unauthorized individuals not affiliated with PNC between February 2016 and May 2017. PNC is not able to confirm which, if any, files or patient information were accessed by these unauthorized individuals, but it is possible that they could have accessed PNC's electronic medical records system containing patient names, addresses, telephone numbers, social security numbers, dates of birth, driver's license numbers, treatment or procedure information, prescription information, and/or healthcare insurance information.

Although PNC unable to confirm that any personally identifying information or patient health information was accessed by unauthorized individuals, out of an abundance of caution and

Attorney General Joseph Foster  
April 25, 2017  
Page 2

because of its commitment to data security and privacy, PNC is notifying all its active and inactive patients about the incident in compliance with the Health Insurance Portability and Accountability Act (HIPAA). In that regard, PNC has a total active and inactive patient population of 176,295 individuals, but only 18 residents of New Hampshire.

Written notice is being mailed to these affected individuals on July 7, 2017, and a sample copy of the notice is enclosed for your records. As an added precaution, PNC is offering all affected individuals 12 months of MyIDCare™ identity theft monitoring and protection from ID Experts®. This product will provide enrolled individuals with a notification of any changes to their credit information, up to \$1,000,000 Identity Theft Insurance Coverage, and access to their credit report. The notice to the affected individuals includes instructions on the use of this product.

PNC also has taken immediate steps in response to learning of this incident, including installing a new firewall, instructing all employees to change all passwords used to log in to its computers, contracting with a third-party IT company to provide additional security and evaluating additional measures to further strengthen its data security. PNC also has reported the incident to law enforcement and will cooperate with any investigation.

I believe this provides you with all information necessary for your purposes and to comply with New Hampshire law. However, if you have any questions or need further information, please contact me.

Very truly yours,

**FREEMAN MATHIS & GARY, LLP**



David A. Cole

DAC/jmr  
Enclosure  
2992885\_1

# Peachtree Neurological Clinic, P.C.

C/O ID Experts  
PO Box 10444  
Dublin, Ohio 43017-4044

To Enroll, Please Call:  
866-690-0768

Or Visit:  
[www.myidcare.com/enrollpeachtree](http://www.myidcare.com/enrollpeachtree)

Enrollment Code:

[XXXXXXXXXX]

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

<<Mail Date>>

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

Thank you for allowing Peachtree Neurological Clinic, PC (“PNC”) to serve your healthcare needs. We take patient privacy seriously and, as part of that commitment, we are sending you this letter to make you aware of a recent data security incident that affected your personal information. Please read this letter carefully.

Recently, PNC’s computer system was infected by a ransomware virus that encrypted our electronic medical records (“EMR”) system containing our patients’ medical records. The ransomware demanded monetary payment from PNC in order to decrypt the files and allow us to regain access to them. We did not pay the ransom to the cyber criminals, but were instead able to restore our files and the functionality of our system through backup records. Subsequent scans of our system show no further sign of the ransomware, and our investigation does not show any indication that the ransomware exfiltrated any data off our system.

However, through our investigation of the incident, we discovered that our computer system previously had been accessed without our knowledge by unauthorized individuals not affiliated with PNC between February 2016 and May 2017. We are not able to confirm which, if any, files or patient information were accessed by these unauthorized individuals, but it is possible that they could have accessed our EMR system and information including your name, address, telephone number, social security number, date of birth, driver’s license number, treatment or procedure information, prescription information, and/or healthcare insurance information.

Please know that PNC takes the protection of your personal information seriously and is taking steps to continue investigating this incident, help mitigate the potential for harm, and prevent this from happening again. In that regard, PNC has reported the incident to law enforcement and is cooperating with its investigation. We also have secured our EMR system and implemented additional security measures to help prevent any unauthorized access.

As an added precaution to help protect your information from potential misuse, we are offering identity theft protection services through ID Experts® and its MyIDCare™ solution at no cost to you. With this protection, MyIDCare will help protect your information from misuse and help you resolve issues if your identity is compromised. We strongly encourage you to register for this free identity theft protection service. To enroll please visit [www.myidcare.com/enrollpeachtree](http://www.myidcare.com/enrollpeachtree) and provide the membership enrollment code listed at the top of this letter.

Your 12-month MyIDCare™ membership will include the following:

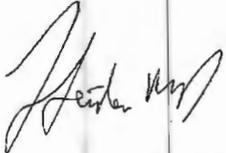
- **Single-Bureau Credit Monitoring** – Monitors any changes reported by Experian Credit Bureau to your credit report.
- **Access to the ID Experts Team** – Access to an online resource center for up-to-date information on new identity theft scams, tips for protection, legislative updates and other topics associated with maintaining the health of your identity.
- **Complete Recovery Services** – Should you believe that you are a victim of identity theft, MyIDCare will work with you to assess, stop, and reverse identity theft issues.

- **Identity Theft Insurance** – In the event of a confirmed identity theft, you may be eligible for reimbursement of up to \$1,000,000 for expenses related to that theft.

Please refer to the enclosed documentation for further instructions from ID Experts® on how to enroll in MyIDCare™, and for additional information on steps you may take to help protect your information from misuse. Please note that you must enroll in MyIDCare™ by **October 7, 2017**.

We are very sorry for any concern or inconvenience this incident has caused or may cause you. If you have any other questions or concerns that you would like to discuss, please call our dedicated, toll-free incident response hotline at **(866) 690-0768**.

Sincerely,

A handwritten signature in black ink, appearing to read "Seiden" followed by a stylized flourish.

Peachtree Neurological Clinic, P.C.  
Dr. Lawrence Seiden, M.D.



### **Enrollment Instructions and Recommended Steps to Help Protect your Information**

**Please Note: You must have a valid United States Social Security Number in order to enroll in credit monitoring services. In addition, credit monitoring is not available for minors under the age of 18, as they should not have a credit history established and are under the age to secure credit. No one is allowed to place a fraud alert on your credit report except you. Please follow the instructions below to place the alert.**

- 1. Website and Enrollment.** Go to [www.myidcare.com/enrollpeachtree](http://www.myidcare.com/enrollpeachtree) and follow the instructions for enrollment using your Enrollment Code provided above. Once you have completed your enrollment, you will receive a welcome letter by email (or by mail if you do not provide an email address when you sign up). The welcome letter will direct you to the MyIDCare Member Website where you will find other valuable educational information.
- 2. Activate the credit monitoring** provided as part of your MyIDCare membership. Credit Monitoring is included in the membership, but you must personally activate it for it to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.
- 3. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies listed below. To obtain a free annual credit report, go to [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any incorrect information on your report, you should report it immediately to the credit reporting agency.
- 4. Report suspected fraud.** You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.
- 5. Place Fraud Alerts** with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating any credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Equifax  
1-800-525-6285  
P.O. Box 740256  
Atlanta, GA 30374  
[www.alerts.equifax.com](http://www.alerts.equifax.com)

Experian  
1-888-397-3742  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

TransUnion  
1-800-680-7289  
P.O. Box 2000  
Chester, PA 19022  
[www.transunion.com](http://www.transunion.com)

It is only necessary to contact ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

- 6. Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above in writing to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. The cost of placing the freeze varies by the state you live

in and for each credit reporting bureau. The Credit Bureau may charge a fee of up to \$5.00 to place a freeze, lift, or remove a freeze. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Theft Complaint Form with the Federal Trade Commission, there may be no charge to place the freeze.

7. **You can obtain additional information** about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

- **California Residents:** Visit the California Office of Privacy Protection, [www.privacy.ca.gov](http://www.privacy.ca.gov), for additional information on protection against identity theft.
- **Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, [www.ag.ky.gov](http://www.ag.ky.gov), Telephone: 1-502-696-5300.
- **Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, [www.oag.state.md.us/Consumer](http://www.oag.state.md.us/Consumer), Telephone: 1-888-743-0023.
- **North Carolina Residents:** Office of the Attorney General of North Carolina, 9001 Mail Service Center, Raleigh, NC 27699-9001, [www.ncdoj.com/](http://www.ncdoj.com/), Telephone: 1-919-716-6400.
- **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, [www.doj.state.or.us](http://www.doj.state.or.us), Telephone: 877-877-9392
- **Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), Telephone: 401-274-4400
- **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://www.consumer.ftc.gov>, 1-877-IDTHEFT (438-4338)