

RECEIVED

JAN 31 2019

CONSUMER PROTECTION

January 25, 2019

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, New Hampshire 03302

Re: Data Security Incident

Dear Attorney General MacDonald:

We represent Dr. DeLuca Dr. Marciano & Associates, P.C. (“DMA”), located at 67 Waterbury Road, Prospect, Connecticut, 06712 with respect to a potential data security incident described in more detail below. DMA takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

1. Nature of the security incident.

On November 29, 2018, DMA discovered that its computer network had been encrypted by ransomware. DMA immediately contacted its information technology team who immediately ensured that further access was denied and then developed a plan to recover the encrypted data. Fortunately backups were available for the affected systems and DMA was able to restore its systems from these backups. However, due to the restoration process, it could not be determined what, if any, information was accessible to the attacker. The systems that were encrypted included systems that contained personal information and protected health information for patients of DMA. This information includes name, address, date of birth, Social Security number, health insurance information, and limited treatment information.

2. Number of New Hampshire residents affected.

A total of twenty-nine (29) New Hampshire residents are known to have been potentially affected by this incident. Notification letters to these individuals were mailed on January 25, 2019, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps taken.

DMA has taken steps to prevent a similar event from occurring in the future, and to protect the privacy and security of potentially affected individuals’ information. This includes, closing all remote access ports, installing stronger anti-virus software and obtaining ransomware protection. DMA has also provided

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston • Indiana • Kentucky
Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • New Jersey • New Orleans • New York • Orlando • Philadelphia • Phoenix • San Diego
San Francisco • Sarasota • Stamford • Virginia • Washington, DC • West Palm Beach • White Plains

wilsonelser.com

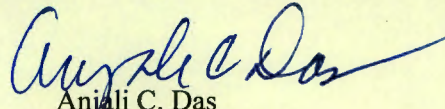
potentially affected individuals with identity theft restoration and credit monitoring services for a period of twenty-four (24) months at no cost to the individuals, through ID Experts.

4. Contact information.

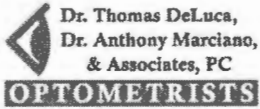
Integrity remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@wilsonelser.com or (312) 821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP


Anjali C. Das

Enclosure.



C/O ID Experts
P.O. Box 10444
Dublin, OH 43017-4044

To Enroll, Please Call:
(844) 322-8213
Or Visit:
<https://ide.myidcare.com/deluca>
Enrollment Code: <<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

January 25, 2019

Dear <<First Name>> <<Last Name>>:

We are writing to inform you of a data security incident at Dr. DeLuca, Dr. Marciano & Associates that may have resulted in the disclosure of your name, Social Security Number (“SSN”), and protected health information (“PHI”). We take the security of your personal information very seriously and sincerely apologize for any inconvenience this incident may cause. This letter contains information about what happened, steps we have taken, and the resources we are making available to you.

On November 29, 2018, we were the victim of a ransomware attack that affected devices on our network that contained electronic medical records. We immediately took action to prevent further infection and restored our network from backup files. However, after a detailed investigation, we learned that some personal information was on the affected devices. This information may have included your name, SSN, and PHI.

Although we have no reason to believe that your information is at risk, out of an abundance of caution, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 24 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling (844) 322-8213 or going to <https://ide.myidcare.com/deluca> and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 5:00 a.m. – 5:00 p.m. Pacific Time. Please note the deadline to enroll is April 28, 2019.

To receive credit services by mail instead of online, please call (844) 322-8213. Additional information describing your services is included with this letter.

We take the security of all information in our control very seriously, and are taking steps to prevent a similar event from occurring in the future. This includes closing all remote access ports, installing stronger anti-virus software, and obtaining ransomware protection. Please know that the protection and security of your personal information is of our utmost priority, and we sincerely regret any concern or inconvenience that this matter may cause you.

If you have any questions, please call (844) 322-8213, Monday through Friday, 5:00 a.m. to 5:00 p.m. Pacific Time.

Sincerely,

A handwritten signature in black ink, appearing to read "Thomas J. DeLuca, O.D.", written in a cursive style.

Thomas J. DeLuca, O.D.
Optometrist
Dr. DeLuca, Dr. Marciano & Associates



Recommended Steps to help Protect your Information

- 1. Website and Enrollment.** Go to <https://ide.myidcare.com/deluca> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
- 2. Activate the credit monitoring** provided as part of your MyIDCare membership. The monitoring included in the membership must be activated 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. Telephone.** Contact MyIDCare at (844) 322-8213 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.
- 4. 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. To obtain a free annual credit report, go to 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 suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that 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 can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your 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:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.alerts.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only 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. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

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 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. There is no cost to freeze or unfreeze your credit files.

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.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, 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, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.