April 24, 2020

Kevin M. Scott
Direct: 312/602-5074
Fax: 312/698-7474
kevin.scott@bryancave.com

BRYAN CAVE LEIGHTON PAISNER LLP
161 North Clark Street Suite 4300
Chicago IL 60601 3315
T: +1 312 602 5000
F: +1 312 602 5050
www.bclplaw.com

Attorney General Gordon MacDonald

Office of the Attorney General
33 Capitol Street
Concord, NH 03302
attorneygeneral@doj.nh.gov

Dear Attorney General MacDonald,

We represent Daniel Bendetowicz MD PA ("DBMP"), a private medical practice specializing in internal medicine, located in Fort Myers, FL, with respect to a data security incident described in more detail below. DBMP takes the security and privacy of the information in its control very seriously, and is taking steps to prevent a similar incident from occurring in the future.

On March 25, 2020, DBMP suffered a ransomware attack on its computer systems. DBMP was able to restore its system and patient health records from its backup system which was untouched, avoiding having to pay the ransom demanded. While DBMP has no reason to believe that the healthcare information was accessed by the attackers, the encrypted system contained electronic healthcare records which include names, addresses, dates of birth, Social Security numbers, medical insurance and related health information.

One (1) New Hampshire resident's personal information may have been encrypted on the server. Notification letters to this resident was mailed by first class mail on April 24, 2020. A sample copy of the notification letter is included with this letter. Although there is no indication of fraudulent activity, in an abundance of caution, residents were offered one year of identity protection (credit monitoring and identity theft restoration) services.

DBMP takes the security of all individuals' information very seriously, and wants to assure you that it is taking steps to prevent a similar event from occurring in the future. Those steps include including increasing DBMP's defenses against these rampant attacks.

DBMP 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.

Very truly yours,

Kevin M. Scott

KMS:llh
Attachment

DANIEL BENDETOWICZ, MD, PA
INTERNAL MEDICINE

<<Date>> (Format: Month Day, Year)

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

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

We are writing to inform you of a data security incident that may have impacted some of your personal information. We take the security of your protected health information very seriously, and we sincerely apologize for any concern this incident may cause. This letter contains information about what happened, actions we have taken to prevent a reoccurrence, and steps you can take to help protect your information.

What happened?
On March 25, 2020, we suffered a ransomware attack on our computer systems. Ransomware is a computer virus that encrypts computer systems until and unless we pay money (i.e., the ransom) demanded by the attackers. Fortunately, we were able to restore our system and your health records from our backup system which was untouched, avoiding having to pay the ransom demanded. These rampant attacks continue to challenge everyone in the business and medical communities. We believe it is likely the attacker only wanted money and not the information on our computers but, in an abundance of caution, we are letting you know that your information was encrypted by the attackers.

What information was involved?
While we have no reason to believe that your healthcare information was accessed by the attackers, the encrypted system contained your electronic healthcare records which include your name, address, date of birth, Social Security number, medical insurance and related health information.

What we are doing.
We take the security of your information seriously and have taken measures to reduce the likelihood of a future cyber-attack, including increasing our defenses against these rampant attacks.

While we do not have any evidence that your information was accessed or acquired by a third party, in an abundance of caution, we are offering the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://[IDMonitoringURL]** to activate and take advantage of your identity monitoring services.
*You have until **[Date]** to activate your identity monitoring services.*
Membership Number: **<<Member ID>>**

Additional information describing your services is included with this letter.

What you can do.
Although we have no reports of misuse of your or anyone's information, we encourage you to follow the instructions in this letter and activate the identity monitoring services we are providing at no cost to you. We also recommend that you review the additional information enclosed, which contains important steps you can take to further safeguard your personal information.

For more information.
If you have any questions, please call 1-???-???-????, Monday through Friday from 9:00 am - 6:30 pm Eastern Time. We appreciate your patience and understanding, and we sincerely apologize for any inconvenience or concern this incident may cause you.

Sincerely,

Daniel Bendetowicz, MD, PA

Additional Important Information

For residents of Hawaii, Illinois, Iowa, Maryland, Michigan, Missouri, North Carolina, Virginia, and Vermont: It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for unauthorized activity. You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa: You are advised to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: You are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of New Mexico: You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident, and that you have rights pursuant to the federal Fair Credit Reporting Act. Please see the contact information for the Federal Trade Commission listed below.

For residents of Illinois, Maryland, North Carolina, and Rhode Island: You can obtain information from the Maryland, North Carolina, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

Rhode Island Office of the Attorney General
Consumer Protection
150 South Main Street
Providence, RI 02903
1-401-274-4400
www.riag.ri.gov

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Ave, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.identitytheft.gov

For residents of Massachusetts and Rhode Island: You have the right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (https://www.experian.com/fraud/center.html), or Transunion (https://www.transunion.com/fraud-victim-resource/place-fraud-alert). 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. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) Proof of current address, such as current utility or telephone bill, bank or insurance statement; (6) legible photocopy of government-issued identification card (state driver's license or ID card, military identification, etc.); and (7) if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013-9544
www.experian.com/freeze/center.html
888-397-3742

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19014-0200
www.transunion.com/credit-freeze
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.

Kroll | A Division of DUFF & PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.