

2018 APR 27 AM 10:35

April 23, 2018

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

Attorney General Joseph A. Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Re: Data Security Incident

Dear Attorney General Foster:

We represent Capital Digestive Care (“CDC”), located in Silver Spring, Maryland, with respect to a potential data security incident described in more detail below. CDC 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 February 23, 2018, CDC was notified that a third-party vendor stored data files on a commercial cloud server without adequate security, which were discovered by an individual who informed CDC of the incident. CDC immediately notified the vendor, who took steps to secure the data files and conducted an investigation to determine what information may have been accessible. As a result of this investigation, it was determined that the information was limited to the “Schedule a Visit” and “Contact” pages on CDC’s website containing personal information patients may have submitted, including their name, address, telephone number, email address, date of birth, and possible health information. The patient “Portal Login” and the “Pay a Bill” pages were not affected and remain secure. No Electronic Medical Records, Social Security numbers, financial account or payment transaction information were involved in this incident.

2. Number of New Hampshire residents affected.

A total number of five (5) New Hampshire residents may have been potentially affected by this incident. Notification letters to these individuals were mailed on April 23, 2018, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps taken.

CDC has taken steps to prevent a similar event from occurring in the future, and to protect the privacy and security of potentially impacted individuals’ information. This includes requiring third-party vendors to

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

2500889v.1

confirm Health Insurance Portability and Accountability Act ("HIPAA") compliance in the secure storage of all personal data. Notice is also being provided to the credit reporting agencies.

4. Contact information.

CDC 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.



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

To <<Name 1>>:

We are writing to inform you of a data security incident involving Capital Digestive Care that may have resulted in the disclosure of your personal information, including your name and limited protected health information. We take the security of all information very seriously, and sincerely apologize for any inconvenience this incident may cause. This letter contains information about steps you can take to protect your information, and resources we are making available to help you.

On February 23, 2018, we were notified that a third-party vendor stored data files on a commercial cloud server without adequate security, which were discovered by an individual who informed us of the incident. We immediately notified the vendor, who took steps to secure the data files and conducted an investigation to determine what information may have been accessible. As a result of this investigation, it was determined that the information was limited to the "Schedule a Visit" and "Contact" pages on our website containing personal information you may have submitted, including your name, address, telephone number, email address, date of birth, and possible health information. The patient "Portal Login" and the "Pay a Bill" pages were not affected and remain secure. No Electronic Medical Records, Social Security numbers, financial account or payment transaction information were involved in this incident.

We do not believe that the limited information could be used adversely, and we have received no reports of the misuse of anyone's data as a result of this incident. However, out of an abundance of caution, we are providing the attached information sheet on steps you can take to protect yourself from the possible misuse of your information.

Identity restoration assistance is available to you for one year from the date of this letter with no enrollment required. If you believe you may be a victim of identity theft please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the following 6-digit telephone pass code **697487** to speak to a dedicated TransUnion representative about your identity theft issue..

We take the security of all information in our control very seriously, and want to assure you that we have taken steps to prevent a similar event from occurring in the future. This includes requiring third-party vendors to confirm Health Insurance Portability and Accountability Act ("HIPAA") compliance in the secure storage of all personal data.

We sincerely regret any concern or inconvenience that this matter may cause you, and remain dedicated to protecting your information. If you have any questions, please do not hesitate to call 855-540-5612, Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely,

Kevin Harlen
Chief Operating Officer

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:

It is required by state laws to inform you that 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 nationwide three 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:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorneys 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.ftc.gov

For residents of Massachusetts:

It is required by state law that you are informed of your 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 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 credit bureaus is below.

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, or 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, 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; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may

charge a small fee to place, lift, or remove a freeze, but is free if you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency. You may obtain a 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
www.freeze.equifax.com
800-525-6285

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

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

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