



STATE OF NH
DEPT OF JUSTICE
2015 SEP 17 AM 11:33

September 11, 2015

Gregory J. Bautista
914.872.7839 (direct)
516.356.8853 (mobile)
Gregory.Bautista@wilsonelser.com

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

Re: Data Security Incident

Dear Attorney General Foster:

We represent Max M. Bayard, MD PC ("Dr. Bayard"), a private medical practice in St. Albans, VT, with respect to a recent security incident involving the potential exposure of certain protected health information described in more detail below. Dr. Bayard takes the security and privacy of the information in his control seriously, and is taking a number of steps to prevent a similar incident from occurring in the future.

1. Nature of the security incident.

On August 5, 2015, Dr. Bayard's offices were broken into and computer devices stolen. As soon as the theft was discovered, Dr. Bayard notified law enforcement and is cooperating with their investigation. Dr. Bayard immediately began an investigation to discover what information was on the devices, and determined that patients' names, Social Security numbers, and other limited treatment-related information may have been on the devices. Although the treatment-related information varies by person, examples include dates of birth, medical insurance information, dates of treatment, types of treatment, and diagnoses.

2. Number of New Hampshire residents affected.

Two (2) New Hampshire residents were affected by the security incident. Notification letters to these individuals were mailed on September 11, 2015, via first class mail. A copy of the notification letter is included with this letter. Notification is also being provided to the credit reporting agencies.

3. Steps you have taken or plan to take relating to the incident.

Immediately upon discovery of the theft, Dr. Bayard changed his firewall password and changed all software-related, login, and email account passwords. Dr. Bayard is also taking steps to prevent this type

1133 Westchester Avenue • White Plains, NY 10604 • p 914.323.7000 • f 914.323.7001

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

wilsonelser.com

1922140v.1

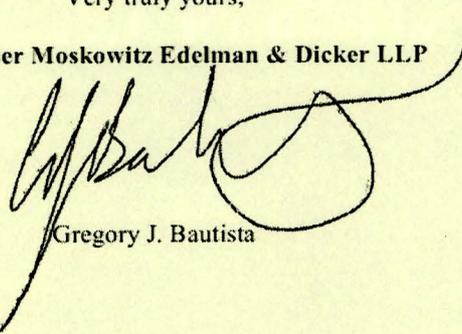
of event from occurring in the future, including installing security cameras, securing the computers in a safe when not in use, encrypting all computers, and reviewing policies and procedures for the secure storage of personal information. Dr. Bayard's staff is being trained on these additional safeguards. Dr. Bayard is also offering potentially impacted individuals credit monitoring and identity protection services at no cost to the individual through AllClear ID.

4. Contact information.

Dr. Bayard remains dedicated to protecting the sensitive information in his systems. If you have any questions or need additional information, please do not hesitate to contact me at Gregory.Bautista@wilsonelser.com or (914) 872-7839.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Gregory J. Bautista

Max M Bayard, MD PC

Processing Center • P.O. Box 141578 • Austin, Texas 78714



01557
JOHN Q. SAMPLE
1234 Main Street
Anytown US 12345-6789

September 11, 2015

Dear John Sample:

We are writing to inform you of a data security incident at Max M. Bayard, MD PC ("Dr. Bayard") that may have resulted in the disclosure of your personal information, including your name, Social Security number, and limited personal health information. 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 steps you can take to protect your information, and resources we are making available to help you.

On August 5, 2015, our offices were broken into and computer devices stolen. As soon as we discovered the theft, we notified law enforcement and are cooperating with their investigation. We also immediately began an investigation to discover what information was on the devices, and determined that your name, Social Security number, and other limited treatment-related information may have been on the devices. Although the treatment-related information varies by person, examples include dates of birth, Medicare/Medicaid enrollment information, dates of treatment, types of treatment, and diagnoses.

Although we are not aware of any misuse of your information, as an added precaution, we have arranged to have AllClear ID protect your identity and monitor your credit for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months:

AllClear SECURE: The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-877-615-3792 and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear PRO: This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.alclearid.com or by phone by calling 1-877-615-3792, using the following redemption code: **Redemption Code**.

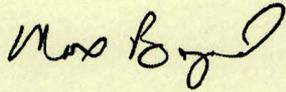
Please note: Additional steps may be required by you in order to activate your phone alerts.



Immediately upon discovery of the theft, we changed the firewall password, and changed all software-related, login, and email account passwords. We are also taking additional steps to prevent this type of event from occurring in the future, including installing security cameras, securing the computers in a safe when not in use, encrypting all computers, and reviewing our policies and procedures for the secure storage of personal information. Our staff is being trained on these additional safeguards.

We deeply regret any inconvenience or concern that this matter may cause you, and remain dedicated to protecting your information. Please call 1-877-615-3792 Monday through Saturday from 9:00 a.m. to 9:00 p.m., Eastern Time, with any questions or concerns.

Sincerely,

A handwritten signature in black ink, appearing to read "Max Bayard". The signature is fluid and cursive, with a large, stylized initial "M" and a long, sweeping tail.

Max Bayard, M.D.

U.S. State Notification Requirements

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 by contacting any one or more of the following national consumer reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-685-1111
www.equifax.com

Experian

P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 6790
Fullerton, CA 92834
1-800-916-8800
www.transunion.com

You may also obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) 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, as well as the Federal Trade Commission.

For residents of Maryland, 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

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 Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/bcp/edu/microsites/idtheft

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 send a request to each consumer reporting agency by certified mail, overnight mail, or regular stamped mail. 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 fee of up to \$5.00 to place a freeze or 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.equifax.com

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze

TransUnion (FVAD)

P.O. Box 2000
Chester, PA 19022
www.transunion.com

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



AllClear Secure Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 12 months of coverage with no enrollment required;
- No cost to you – ever. AllClear Secure is paid for by the participating Company.

Services Provided

If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Secure is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period

Service is automatically available to you with no enrollment required for 12 months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud events that occurred prior to your Coverage Period are not covered by AllClear Secure services.

Eligibility Requirements

To be eligible for Services under AllClear Secure coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim

If you become a victim of fraud covered by the AllClear Secure services (an "Event"), you must:

- notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- provide proof of eligibility for AllClear Secure by providing the redemption code on the notification letter you received from the sponsor Company;
- fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage Under AllClear Secure Does Not Apply to the Following:

Any expense, damage or loss:

- due to
 - any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
 - any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation");
- incurred by you from an Event that did not occur during your coverage period; or
- in connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Secure coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation, fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Secure is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of Secure coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy

If for any reason you wish to have your information removed from the eligibility database for AllClear Secure, please contact AllClear ID:

E-mail support@allclearid.com	Mail AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	Phone 1.855.434.8077
---	--	--------------------------------

