



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

RECEIVED
JUN 18 2018
CONSUMER PROTECTION

Christopher J. DiIenno
Office: 267-930-4775
Fax: 267-930-4771
Email: cdiienzo@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

June 14, 2018

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident

Dear Gordon J. MacDonald

We represent Med Associates, Inc. ("Med Associates"), located at 13 British American Blvd, Latham, NY 12110, and are writing to notify your office of an incident that may affect the security of some personal information relating to 10 New Hampshire residents. By providing this notice on behalf of various Data Owners (*Exhibit A*), Med Associates does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about March 22, 2018, Med Associates became aware of unusual activity relating to an employee's workstation occurring that same day. Med Associates immediately began investigating with our IT vendor and subsequently retained a leading third-party forensic investigation firm to assist with our investigation. It was determined that the unauthorized party accessed the workstation and through that, may have had access to certain personal and protected information.

The information that could have been subject to unauthorized access includes patient name, date of birth, address, dates of service, diagnosis codes, procedure codes and insurance information, including insurance ID Number.

Notice to New Hampshire Residents

On or about June 14, 2018, Med Associates provided written notice of this incident to all affected individuals, which includes 10 New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit B*.

Other Steps Taken and To Be Taken

Upon discovering the event, Med Associates moved quickly to investigate and respond to the incident, assess the security of Med Associates systems and secure the impacted workstation. Med Associates notified Data Owners on May 18, 2018. Med Associates posted notice of the incident on its website on May 22, 2018. Med Associates implemented even more stringent information security standards and increased staff training on data privacy and security.

Med Associates is providing access to credit monitoring services for one (1) year, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Med Associates is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Med Associates is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4775.

Very truly yours,



Christopher J. DiIenno of
MULLEN COUGHLIN LLC

CJD/alc
Enclosure

EXHIBIT A

Data Owner	Contact Person	Address Line 1	City	State	Zip Code	Impacted Population
Albany Advance Imaging, PLLC	Paul J. Gordon - Practice Administrator	3 Atrium Drive	Albany	NY	12205	1
Adirondack Pathology, PC	Dr. Jayant Paranjpe	100 Park Street	Glen Falls	NY	12801	1
William J. Feeney, MD, PLLC	Dr. William Feeney	582 New Loudon Road	Latham	NY	12110	3
Maplewood Pathology, PC	Dr. Lisle A. Eaton, Jr - President	315 South Manning Blvd	Albany	NY	12208	3
Theta Pattison, MD	Dr. Theta Pattison	2508 Western Ave	Altamont	NY	12009	1
Edwin F. Williams III, MD	Dr. Edwin Williams III	1072 Troy-Schenectady Road	Latham	NY	12110	1

EXHIBIT B



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>>

Re: Notice of Data Security Incident

Dear <<Name 1>>:

Med Associates, Inc. processes claims for medical providers located in and around Albany, NY. As a patient of one or more medical providers who Med Associates, Inc. currently provides, or has provided services to, we are writing to inform you of an incident that may have involved your patient information. We have no evidence that any patient information was specifically accessed or used in any way. However, we are unable to definitively rule that out, therefore, we are providing this information regarding the data incident and steps we have taken since discovery.

What Happened? On March 22, 2018, Med Associates became aware of unusual activity relating to an employee's workstation occurring that same day. Med Associates immediately began investigating with our IT vendor and subsequently retained a leading third-party forensic investigation firm to assist with our investigation. It was determined that the unauthorized party accessed the workstation and through that, may have had access to certain personal and protected information.

What Information was Involved? While our investigation is ongoing, we have determined that the information that may have been accessible from the workstation included patient name, date of birth, address, dates of service, diagnosis codes, procedure codes and insurance information, including insurance ID Number. There was no banking or credit card information contained on or accessible from the workstation.

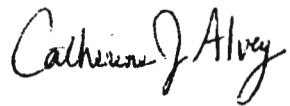
What We Are Doing. The privacy and security of information in our possession is one of our highest priorities. Upon learning of this incident, we immediately secured the impacted workstation, implemented even more stringent information security standards and have increased staff training on data privacy and security.

Again, we have no indication that information was accessed or misused, however, we recommend you check any statements you receive from your health insurer. If you see charges for services you did not receive, please contact the insurer immediately. As an added precaution, we are offering you access to one year of credit monitoring and identity theft restoration services through TransUnion at no cost to you. Please review the instructions contained in the attached *Steps You Can Take to Protect Your Information* for additional information.

What You Can Do. You can review the enclosed *Steps You Can Take to Protect Your Information*, which contains information on what you can do to better protect against the possibility of identity theft and fraud should you feel it is appropriate to do so.

For More Information. We sincerely regret any inconvenience or concern this may have caused. We understand you may have questions that are not answered in this letter. To ensure your questions are answered in a timely manner, you can call our dedicated assistance line at 855-206-9883, Monday through Friday, 9:00 a.m. to 9:00 p.m. ET.

Sincerely,

A handwritten signature in black ink that reads "Catherine J. Alvey". The signature is written in a cursive style with a large, stylized initial "C".

Catherine Alvey
President

Encl.

Steps You Can Take to Protect Your Information

Complimentary Credit Monitoring Enrollment Instructions

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for <<Insert one year>> provided by TransUnion Interactive, a subsidiary of TransUnion[®], one of the three nationwide credit reporting companies.

To enroll in this service, go to the *myTrueIdentity* website at **www.mytrueidentity.com** and in the space referenced as "Enter Activation Code", enter the following 12-letter Activation Code <<Insert Unique 12- letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, 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 <<Insert static 6-digit Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Insert Date>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain <<Insert one year>> of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

Monitor Your Accounts

Credit Reports. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your free credit reports and explanation of benefits forms for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Fraud Alerts. At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below:

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

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

TransUnion
P.O. Box 2000
Chester, PA 19016
800-680-7289
www.transunion.com

Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from \$3 to \$15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111

<https://www.freeze.equifax.com>

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/

TransUnion

P.O. Box 2000
Chester, PA 19016
1-888-909-8872

[www.transunion.com/credit-freeze/
place-credit-freeze](http://www.transunion.com/credit-freeze/place-credit-freeze)

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General, as well as the credit reporting agencies listed above. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be reported to law enforcement, the Federal Trade Commission, and your state Attorney General. **For Maryland residents,** the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. **For 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 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. We encourage you to 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. **For North Carolina residents,** the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov. **For Rhode Island residents,** the Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. A total of 19 Rhode Island residents may be impacted by this incident. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or 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 they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed as the result of a law enforcement investigation.