LEWIS BRISBOIS BISGAARD & SMITH LLP

Lindsay B. Nickle
2100 Ross Avenue, Suite 2000
Dallas, Texas 75201
Lindsay.Nickle@lewisbrisbois.com
Direct: 214.722.7141

June 18, 2020

VIA EMAIL
Attorney General Gordon MacDonald
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

We represent American Medical Technologies ("AMT") a medical provider located in Irvine, California, with regard to a recent data security incident described in greater detail below. This letter is being sent on behalf of AMT because personal information belonging to New Hampshire residents may have been affected by a recent data security incident.

1. Nature of the security incident.

On or about December 17, 2019, AMT discovered suspicious activity within an employee's email account. AMT immediately engaged a third-party forensic firm to perform an investigation into their email tenant. After an extensive and comprehensive investigation and data mining process, on May 14, 2020, AMT learned that certain patients' personal information may have been available to the attacker during the incident. The information that may have been accessed includes names, Social Security numbers, medical record numbers, diagnosis information, health insurance policy or individual subscriber numbers, medical history information, HIPAA account information, driver's license/state identification numbers, and/or taxpayer ID numbers. Notably, AMT is not aware of any misuse of this information as a result of this incident.

2. Number of New Hampshire residents affected.

Approximately 81 residents of New Hampshire may have been affected by this incident. AMT will be notifying the potentially affected New Hampshire residents on or about June 18, 2020, via U.S. mail. A sample copy of the notification letter is being provided with this correspondence.

3. Steps taken relating to the incident.

AMT engaged two separate information security companies to review their email systems. AMT implemented improvements per their recommendations to increase the security of their email systems. AMT also implemented additional safeguards to improve data security on their web server infrastructure. In addition, AMT is offering identity theft protection services through ID Experts® to provide affected patients with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services.

4. Contact Information.

AMT remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at (214) 722-7141 or by e-mail at lindsay.nickle@lewisbrisbois.com.

Please let me know if you have any questions.

Very truly yours,

Lindsay B. Nickle of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Sample Notification Letter

C/O ID Experts
P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
833-579-1109
Or Visit:
https://app.myidcare.com/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

<<FirstName>> <<LastName>>
<<Address1>><<Address2>>
<<City>>, <<State>> <<Zip Code>>

June 18, 2020

Re: Notification of Data Security Incident

Dear <<FirstName>> <<LastName>>,

We are writing to inform you of a potential data security incident involving American Medical Technologies ("AMT") that may have involved your personal information. At AMT, we take the privacy and security of all information we collect and store very seriously.

What Happened? On or about December 17, 2019 we discovered suspicious activity within an employee's email account. We immediately engaged a third-party forensic firm to perform an investigation into our email tenant. After an extensive and comprehensive investigation and data mining process, on May 14, 2020, we learned that your personal information may have been available to the attacker during the incident. We are sending you this letter to notify you about the incident and provide information about steps you can take to protect your information.

What Information Was Involved? Based on our investigation, your Social Security number, medical record number, diagnosis information, health insurance policy or individual subscriber number, medical history information, HIPAA account information, driver's license/state identification number, or taxpayer ID number, may have been impacted by this incident.

What We Are Doing. We engaged two separate information security companies to review our email systems. We implemented improvements per their recommendations to increase the security of our email systems. We have also implemented additional safeguards to improve data security on our web server infrastructure. In addition, 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: 12 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.

What You Can Do.. We encourage you to enroll in the free credit monitoring and insurance services by using the enrollment code at the top of this letter and going to https://app.myidcare.com/account-creation/protect or calling 833-579-1109. MyIDCare experts are available Monday through Friday from 8 am - 8 pm Central Time. Please note the deadline to enroll is September 18, 2020.

For More Information. You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 833-579-1109 or go https://app.myidcare.com/account-creation/protect for assistance or for any additional questions you may have.

Sincerely,

Jeremy White

Jeremy White
Chief Privacy Officer
American Medical Technologies

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-800-909-8872	1-888-397-3742	1-800-685-1111	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	www.annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. You also have the right to obtain any police report filed in regard to this incident. Contact information for the FTC is: **Federal Trade Commission,** 600 Pennsylvania Ave, NW, Washington, DC 20580, www.consumer.ftc.gov and www.ftc.gov/idtheft, 1-877-438-4338. Residents of New York, Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

New York Attorney General Bureau of Internet and Technology Resources	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
28 Liberty Street	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
New York, NY 10005	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
ifraud@ag.ny.gov	www.oag.state.md.us	www.ncdoj.gov	www.riag.ri.gov
1-212-416-8433	1-888-743-0023	1-877-566-7226	401-274-4400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf