DrinkerBiddle&Reath LLP

John J. Brudz
Partner
202-230-5195
202-842-8465
Jay.Brudz@dbr.com

Law Offices
1500 K Street, NW
Suite 1100
Washington, DC
20005-1209

202-842-8800
202-842-8465 fax
www.drinkerbiddle.com

CALIFORNIA
DELAWARE
ILLINOIS
NEW JERSEY
NEW YORK
PENNSYLVANIA
TEXAS
WASHINGTON D.C.

June 11, 2018

Attorney General Gordon MacDonald
Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

STATE OF NH
DEPT OF JUST
2018 JUN 12 AM 10:15

Re: Notice of Data Breach

Dear Attorney General MacDonald:

Please be advised that our firm, Drinker Biddle & Reath LLP represents Boston Biomedical, Inc. (the "Company"), headquartered in Cambridge, Massachusetts. Since its founding in 2006, Boston Biomedical has been leading advances in the development of cancer treatments.

A recent IT investigation revealed that the Company was the target of a cyberattack seeking confidential business information. Upon discovery of a suspected Business Email Compromise attack, Boston Biomedical promptly activated its incident response plan, including engagement of a cybersecurity firm and federal law enforcement.

From the initial investigation findings, stolen credentials were used to access an employee's work email account. The forensic investigation indicated that the earliest access of the account was on January 11, 2018. The attack was discovered and contained on May 2, 2018. During the investigation, it was determined that the mailbox in question contained attachments housing certain personal information of some current and former employees of the Company, as well as a several contractors. Also identified were a limited number of instances where messages containing personal information were transmitted via email to an unknown third party during this time period.

Based on the facts known to Boston Biomedical at this time, we believe that the stolen credentials (i.e. username and password) were used to access an employee's work email account beginning on January 11, 2018. The account compromised was of an employee whose job function included occasionally handling personal information. The information found in emails in the account included W-9, I-9, and other employment forms, containing names, addresses, dates of birth, Social Security numbers, and in some cases passport numbers, along with other types of personal information of approximately 252 current and former employees and contractors total. Specifically, we believe four of these individuals are New Hampshire residents.

Upon accessing the compromised email account, the criminals used rules to allow mail-forwarding third-party email addresses, which were disabled on May 2, 2018 – terminating any unauthorized access. While it is not clear what emails were in fact accessed, the investigation has identified three instances where messages containing personal information were transmitted to an unknown third-party email account.

There has been no indication that the information transmitted or accessed contained any clinical, product, patient, or proprietary data. Moreover, the investigation suggests that the incident did not involve a breach of information technology, firewalls, networks, and/or databases. The security surrounding these systems have not been compromised.

Boston Biomedical takes privacy and data security seriously and intends to use this event as a driver to reinvigorate our data governance processes for safeguarding personnel data. We are currently engaged in notifying personnel affected by this situation and assisting with them with the remediation process. Since the data breach was discovered, the Company has worked closely with a leading cybersecurity firm and federal law enforcement to investigate. In addition, we are working to make whatever changes may be necessary to strengthen our information systems against attack, improve our email systems' authentication process, and invest in enhanced network monitoring capabilities.

The Company sent a notification letter by mail to all affected personnel (**see Appendix A enclosed**) on June 8, 2018, which included instructions to obtain information about the breach and options available to them, including an offer for 12 months of free fraud detection and identity theft protection services through InfoArmor (available at: www.infoarmor.com/dataprotection2018), along with a dedicated Company contact for any questions or concerns regarding the data breach (available at: privacyquestions@bostonbiomedical.com). The letter includes additional information such as governmental resources and how to contact the major credit reporting agencies.

Please feel free to contact me at jay.brudz@dbr.com or 202-230-5195 if you have any questions or concerns.

Very truly yours,

John J. Brudz

cc. Andrea L. Kocharyan, VP, Legal Affairs – Boston Biomedical, Inc.

Enclosure

APPENDIX A

RE: NOTICE OF DATA BREACH

June 8, 2018

Dear _____:

Maintaining the privacy and security of your personal information and the Company's proprietary information is of the utmost importance at Boston Biomedical. It has recently come to our attention that personal information of some personnel may have been accessed by an unknown third party. Boston Biomedical is committed to the security of your personal information and is taking the appropriate steps to remedy the security breach.

What Happened: A recent IT investigation revealed that Boston Biomedical was the target of a cyberattack seeking confidential business information of Boston Biomedical. Upon discovery of a suspected Business Email Compromise attack, Boston Biomedical promptly activated its incident response plan, including engagement of a cybersecurity firm and cooperation with federal law enforcement.

From the initial investigation findings, stolen credentials were used to access an employee's work email account. The forensic investigation indicated that the earliest access of the account was on January 11, 2018. The attack was discovered and contained on May 2, 2018. During the investigation, it was determined that the mailbox in question contained attachments housing certain personal information of some current and former employees of the Company, as well as a several contractors. Also identified were a limited number of instances where messages containing personal information were transmitted via email to an unknown third party during this time period.

What Information Was Involved: Based on the facts known to Boston Biomedical at this time, we believe that the stolen credentials (i.e. username and password) were used to access an employee's work email account, beginning on January 11, 2018. The account compromised was of an employee whose job function included occasionally handling personal information. The information found in emails in the account included W-9, I-9, and other employment forms, containing names, addresses, dates of birth, Social Security numbers, and in some cases passport numbers, along with other types of personal information of approximately 252 current and former employees and contractors.

Upon accessing the compromised email account, the criminals used rules to allow mail-forwarding third-party email addresses, which were disabled on May 2, 2018 – terminating any unauthorized access. While it is not clear what emails were in fact accessed, the investigation has identified three instances where messages containing personal information were transmitted to an unknown third-party email account.

There has been no indication that the information transmitted or accessed contained any clinical, product, patient, or proprietary data. Moreover, the investigation suggests that the incident did not involve a

breach of information technology, firewalls, networks, and/or databases. The security surrounding these systems have not been compromised and remains secure.

What We Are Doing: Boston Biomedical takes privacy and data security seriously and intends to use this event as a driver to reinvigorate our data governance processes for safeguarding personnel data. We are currently engaged in notifying personnel affected by this situation and assisting with them with the remediation process.

Since the security breach was discovered, Boston Biomedical has worked closely with a leading cybersecurity firm and federal law enforcement to investigate. In addition, we are working to make whatever changes may be necessary to strengthen our information systems against attack, and are improving our email systems' authentication process and investing in enhanced network monitoring capabilities to protect the security of your information.

As a precaution, we are offering any affected current or former employees and contractors 12 months of free fraud detection and identity theft protection through InfoArmor's specialized monitoring service. To learn more and to take advantage of the service please visit our exclusive online enrollment portal: www.infoarmor.com/dataprotection2018. Any questions or concerns can be referred to Boston Biomedical by emailing privacyquestions@bostonbiomedical.com.

What You Can Do: The security of your personal information is important to us, and we are working hard to ensure that it is protected. We encourage any personnel notified about the security breach to remain vigilant by reviewing your credit report and your financial account statements for any unauthorized activity. If you suspect any unauthorized activity, immediately contact us and your financial institutions.

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, there are several thing you can do: (i) request a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies, listed below; (ii) contact the Federal Trade Commission and/or the Attorney General's consumer protection office in your state; (iii) obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes; and/or (iv) contact your local law enforcement authorities to file a police report or obtain a copy of the police report. Additional resources, including state-specific guidance, are listed below.

We apologize wholeheartedly to our personnel and will continue to be vigilant against future incidents. If you have any further questions, please contact privacyquestions@bostonbiomedical.com.

Sincerely,

Andrea L. Kocharyan
VP, Legal Affairs

ADDITIONAL RESOURCES

To obtain your free annual credit report, please visit www.annualcreditreport.com or call 1-877-322-8228.

Equifax	Experian	TransUnion
P.O. Box 740256 Atlanta, GA 30374 1-866-349-5191 www.equifax.com	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com	P.O. Box 105281 Atlanta, GA 30348 1-888-909-8872 www.transunion.com

Federal Trade Commission: Contact information for the Federal Trade Commission is as follows: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.ftc.gov/idtheft, or call 1-877-IDTHEFT (438-4338).

For California Residents: You may contact the California Attorney General's Office at California Department of Justice, Attn: Office of Privacy Protection, P.O. Box 944255, Sacramento, CA 94244, or call 916-322-3360. You can also obtain more information about the steps you can take to avoid identity theft from the Attorney General's website: www.oag.ca.gov.

For Maryland Residents: You may contact the Maryland Attorney General's Office at 200 St. Paul Place, Baltimore, MD 21202, or call 1-888-743-0023. You can also obtain more information about the steps you can take to avoid identity theft from the Attorney General's website: www.oag.state.md.us.

For Rhode Island Residents:

- Under Rhode Island law, you have the right to obtain a copy of any police report.
- Security Freeze: Rhode Island law also allow consumers to request a security freeze. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Be mindful 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.
- The fee for placing a security freeze on a credit report is $5.00. If you are a victim of identity theft and submit a valid investigative report or complaint with a law enforcement agency, the fee will be waived. In all other instances, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze. If you have not been a victim of identity theft, you will need to include payment to the credit reporting agency to place, lift, or remove a security freeze by check, money order, or credit card.
- To place a security freeze on your credit report, you must send a written request to each of the three major reporting agencies by regular, certified, or overnight mail at the addresses below:
    - **Equifax Security Freeze**, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com, or call 1-800-685-1111.

- **Experian Security Freeze**, P.O. Box 9554, Allen, TX 75013, www.experian.com, or call 1-888-397-3742
- **TransUnion Security Freeze**, P.O. Box 2000, Chester, PA 19022, www.transunion.com, or call 1-888-909-8872.

- In order to request a security freeze, you will need to provide the following information:
  - Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
  - Social Security number;
  - Date of birth;
  - If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
  - Proof of current address such as a current utility bill or telephone bill;
  - A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
  - If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.
- The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique PIN or password or both that can be used by you to authorize the removal or lifting of the security freeze.
- To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.
- To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

For North Carolina Residents: You may contact the North Carolina Attorney General's Office at 9001 Mail Service Center, Raleigh, NC 27699, or call 919-716-6400. You can also obtain more information about the steps you can take to avoid identity theft from the Attorney General's website: www.ncdoj.gov.