



Alyssa R. Watzman  
1700 Lincoln Street, Suite 4000  
Denver, Colorado 80203  
Alyssa.Watzman@lewisbrisbois.com  
Direct: 720.292.2052

December 21, 2022

**Via E-Mail**

Attorney General Brian E. Frosh  
Office of the Attorney General  
Attn: Security Breach Notification  
200 St. Paul Place  
Baltimore, MD 21202  
Email: [Idtheft@oag.state.md.us](mailto:Idtheft@oag.state.md.us)

Re: Notice of Data Security Incident

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP ("Lewis Brisbois") represents ABM Therapeutics Corporation ("ABM") in connection with a data security incident described in greater detail below.

**1. Nature of the security incident.**

On June 2, 2022, ABM identified suspicious activity associated with one employee email account. In response, ABM took immediate steps to secure its email environment and later launched an investigation. In so doing, ABM engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been accessed or acquired without authorization as a result. On November 4, 2022, ABM received confirmation that one employee email account was accessed without authorization. On December 15, 2022, ABM learned that personal information belonging to certain individuals associated therewith may have been impacted. ABM then took steps to identify current mailing addresses to effectuate notification.

The information that may have been accessible by the malicious actor(s) responsible for this incident includes name and Social Security number.

**2. Number of Maryland residents affected.**

ABM notified one Maryland resident of this incident via first class U.S. mail on December 21, 2022. A sample copy of the notification letter is included with this correspondence.

**3. Steps taken relating to the Incident.**

As soon as ABM discovered this incident, ABM took steps to secure its email environment and

December 21, 2022

Page 2

launched an investigation to determine what happened and whether personal information had been accessed or acquired without authorization. ABM has also implemented additional safeguards to help ensure the security of its email environment and to reduce the risk of a similar incident occurring in the future.

Importantly, while ABM is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, ABM is providing complimentary identity protection services to notified individuals through IDX - a data breach and recovery services expert.

#### **4. Contact information.**

ABM 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 Lewis Brisbois.

Best regards,



Alyssa R. Watzman

LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Sample Notification Letter



4445 Eastgate Mall, Suite 200  
San Diego, CA 92121

<<First Name>> <<Last Name>>  
<<Address1>> <<Address2>>  
<<City>>, <<State>> <<Zip>>

To Enroll, Please Call:  
1-800-939-4170

Or Visit:  
<https://app.idx.us/account-creation/protect>

Enrollment Code: <<XXXXXXXX>>

<<Date (Format: Month Day, Year)>>

Subject: Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

I am writing to inform you of a data security incident experienced by ABM Therapeutics Corporation (“ABM”) that may have affected your personal information. ABM takes the privacy and security of all personal information within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your personal information.

**What Happened?** On June 2, 2022, ABM identified suspicious activity associated with one employee email account. In response, ABM took immediate steps to secure its email environment and later launched an investigation. In so doing, ABM engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been accessed or acquired without authorization as a result. On November 4, 2022, ABM received confirmation that one employee email account was accessed without authorization. On December 15, 2022, ABM learned that your personal information may have been impacted as a result which is the reason for this notification. Please note that ABM has no evidence of the misuse or attempted misuse of any potentially impacted information.

**What Information Was Involved?** The information potentially impacted in connection with this incident included your name as well as your Social Security number.

**What Are We Doing?** As soon as ABM discovered this incident, ABM took the steps described above. In addition, ABM implemented measures to enhance the security of its email environment in an effort to minimize the risk of a similar incident occurring in the future. ABM also notified the Federal Bureau of Investigation of this incident and will provide whatever cooperation is necessary to hold the perpetrator(s) accountable.

Although ABM has no evidence of the misuse of any potentially impacted information, ABM is providing you with information about steps that you can take to help protect your personal information and is offering you complimentary identity protection services through IDX – a data breach and recovery services expert. These services include 12 months of credit<sup>1</sup> and dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services.

The deadline to enroll in these services is April 1, 2023. With this protection, IDX will help to resolve issues if your identity is compromised.

---

<sup>1</sup> To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

**What You Can Do:** You can follow the recommendations on the following page to help protect your personal information. ABM also encourages you to enroll in the complementary services being offered to you through IDX by using the enrollment code provided above.

**For More Information:** Further information about how to protect your personal information appears on the following page. If you have questions about this incident, please call Susan Xu at 760-672-5651. If you need assistance with enrollment in the complimentary services being offered to you, please call IDX at 1-800-939-4170 from 6:00 A.M. to 6:00 P.M. Pacific Time, Monday through Friday (excluding holidays).

Please accept my sincere apologies and know that ABM takes this matter very seriously and deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in cursive script, appearing to read 'Susan Xu', written in dark ink.

Susan Xu, Accounting  
ABM Therapeutics Corporation

## STEPS YOU CAN TAKE TO HELP 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 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

**Equifax**

P.O. Box 105851  
Atlanta, GA 30348  
1-800-525-6285  
[www.equifax.com](http://www.equifax.com)

**Experian**

P.O. Box 9532  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

**TransUnion**

P.O. Box 1000  
Chester, PA 19016  
1-800-916-8800  
[www.transunion.com](http://www.transunion.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 one year. 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:** 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.

**Federal Trade Commission**

600 Pennsylvania Ave, NW  
Washington, DC 20580  
[consumer.ftc.gov](http://consumer.ftc.gov), and  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)  
1-877-438-4338

**Maryland Attorney General**

200 St. Paul Place  
Baltimore, MD 21202  
[oag.state.md.us](http://oag.state.md.us)  
1-888-743-0023

**New York Attorney General**

Bureau of Internet and Technology  
Resources  
28 Liberty Street  
New York, NY 10005  
1-212-416-8433

**North Carolina Attorney General**

9001 Mail Service Center  
Raleigh, NC 27699  
[ncdoj.gov](http://ncdoj.gov)  
1-877-566-7226

**Rhode Island Attorney General**

150 South Main Street  
Providence, RI 02903  
<http://www.riag.ri.gov>  
1-401-274-4400

**Washington D.C. Attorney General**

441 4th Street, NW  
Washington, DC 20001  
[oag.dc.gov](http://oag.dc.gov)  
1-202-727-3400

**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 other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.