LEWIS BRISBOIS BISGAARD & SMITH LLP

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

April 20, 2018

VIA ELECTRONIC SUBMISSION
Attorney General Joseph Foster
Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
E-Mail: DOJ-CPB@doj.nh.gov

Re: Notification of Data Security Incident

Dear Attorney General Foster:

We represent American Esoteric Laboratories ("AEL") in connection with a recent data security incident which is described in greater detail below. AEL takes the security and privacy of the information in its control very seriously and is taking steps to prevent a similar incident from occurring in the future.

1. Nature of the security incident.

On October 15, 2017, a laptop issued to an AEL employee was stolen. The laptop may have contained personal and protected health information belonging to some AEL patients and their payment guarantors. Upon learning of the incident, AEL disabled the stolen laptop's access to its computer network and reported the laptop theft to the local police. AEL also conducted an investigation to determine what information may have been stored on the laptop. The information may have included names, addresses, Social Security numbers, dates of birth, health insurance information, and/or medical treatment information.

2. Number of New Hampshire residents affected.

AEL notified 3 New Hampshire residents regarding this data security incident. Notification letters were mailed via first class U.S. mail on April 20, 2018. A sample copy of the notification letter is included with this letter.

3. Steps taken relating to the incident.

AEL has taken affirmative steps to prevent a similar situation from arising in the future and to protect the privacy and security of all sensitive information in its possession. These steps include installing encryption technology, updating relevant policies and procedures, and retraining staff. In addition, potentially impacted individuals have been offered twelve (12) months of credit monitoring and identity protection services through ID Experts® at no cost.

4. Contact information.

AEL is dedicated to protecting the sensitive information that is 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.

Sincerely,

Lindsay B. Nickle of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure

AMERICAN ESOTERIC LABORATORIES
A Sonic Healthcare Company

C/O ID Experts
PO Box 10444
Dublin, OH 43017 - 4044

To Enroll, Please Call:
(888) 285-9795
Or Visit:
https://ide.myidcare.com/AELprotect
Enrollment Code: <<Code>>

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

Subject: Notice of Data Breach

April 20, 2018

Dear <<First Name>> <<Last Name>>:

I am writing to inform you of a data security incident that may have involved your personal information. American Esoteric Laboratories ("AEL") takes the privacy and security of your personal information very seriously and regrets any concern that this incident may cause you. This letter contains information about steps that you can take to protect your personal information and about resources that we are making available to help you.

What Happened?

On October 15, 2017, a laptop issued to one of AEL's employees was stolen. The laptop may have contained personal health information ("PHI") belonging to some AEL patients. Upon learning of the incident, AEL disabled the employee's email account and the stolen laptop's access to its computer network. AEL also reported the laptop theft to the local police. While AEL has no evidence that your personal information has been inappropriately accessed or acquired without authorization, out of an abundance of caution, AEL is informing you of the incident and providing you with the resources in this letter.

What Information Was Involved?

Our investigation indicates that some of your personal information, which may include your name, address, Social Security number, date of birth, health insurance information, or medical treatment information, may have been stored on the laptop.

What You Can Do.

While we are not aware of the misuse of your information, to help relieve concerns and restore confidence following this incident, we have secured the services of ID Experts®, a data breach and recovery services expert, to provide identity theft protection services for one year. These services include 12 months of credit monitoring, a $1,000,000 insurance reimbursement policy, exclusive educational materials, and fully managed identity theft recovery services. Please note that the deadline to enroll is July 21, 2018. To receive these identity theft protection services, you must be over the age of 18, 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. In addition, we recommend that you review the additional information provided with this letter about steps you can take to protect your personal information. If you are not over the age of 18, please contact ID Experts® to discuss enrolling in alternative fraud consultation and identity theft restoration services.

What Are We Doing?

We take the security of all personal information that we store in our systems very seriously and we are taking steps to enhance the security of such information in order to prevent similar incidents from occurring in the future. These steps include increasing the security of our systems and networks through the use of encryption technology, updating our policies and procedures, and retraining our staff.

For More Information.

We sincerely regret any inconvenience or concern that this matter may cause you and we remain dedicated to protecting your information. If you have questions or need assistance, please call (888) 285-9795 from 8:00 A.M. to 8:00 P.M. ET, Monday through Friday.

Sincerely,

Fran W. Sorrell
Director of Compliance

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 and review 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 should also 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 (the "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 also contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-877-322-8228
www.equifax.com	www.experian.com	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 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: In some U.S. states, you have the right to put a security freeze on your credit file. 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. If you request a security freeze from a consumer reporting agency there may be a fee up to $10 to place, lift or remove the security freeze. 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 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. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.