



AMERICAN ESOTERIC LABORATORIES

C/O ID Experts
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: Data Security Incident

Dear <<Name 1>>:

We are writing to inform you of a data security incident experienced by Retrieval Masters Creditors Bureau d/b/a American Medical Collection Agency (“AMCA”), one of American Esoteric Laboratories’ (“AEL”) vendors. This incident may have involved your personal information. At AEL we take the privacy and security of our patients’ information very seriously. 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 Happened?

On May 15, 2019, we were notified that AMCA experienced a data security incident that involved the payment page on AMCA’s website and unauthorized access to an AMCA database containing information belonging to AEL’s patients. AMCA is a vendor that assisted AEL with the collection of unpaid accounts. The security of AEL’s systems was not affected by this incident. Upon receiving notification about this incident, we immediately began an investigation to identify the affected individuals and the nature of affected information. We are utilizing cyber security experts to assist us in our investigation. Although we are unaware of the misuse of any of your personal information, out of an abundance of caution, we are notifying you about this incident and providing you information about steps you can take to protect your personal information.

What Information Was Involved?

Your name, address, phone number, date of birth, date(s) of service, balance information, and treatment provider information may have been involved in the incident.

What We Are Doing And What You Can Do.

Since receiving notification about the incident, AEL has stopped using AMCA for collection efforts. In addition, although we are not aware of any misuse of your information, we are providing you with this notification about the incident. The following pages also include information about steps you can take to protect your personal information as a precautionary measure.

For More Information.

The privacy and protection of patient information is a top priority at AEL, and we appreciate your patience and loyalty through this incident. If you have any questions, please do not hesitate to call 833-297-6408 from 9:00 a.m. to 9:00 p.m., Eastern Time, Monday through Friday or you can go to the informational website <https://ide.myidcare.com/AEL>.

Please be advised that effective immediately, payments should no longer be made to AMCA. If you have an outstanding balance, please contact us directly at 866-365-8080.

Sincerely,

A handwritten signature in black ink that reads "David I Smalley". The signature is written in a cursive style with a long horizontal flourish at the end.

David Smalley, Ph.D
President

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 for the next twelve to twenty-four months 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. If you detect any information related to fraudulent transactions, you should notify the credit reporting agency that issued the report and have it deleted. You can also 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	Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 1000 Chester, PA 19016 1-877-322-8228 www.transunion.com	Free Annual Report P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 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: 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. 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 are encouraged to report suspected identity theft to the FTC. You may also report suspected identity theft to local law enforcement, including 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 600 Pennsylvania Ave, NW Washington, DC 20580 consumer.ftc.gov, and www.ftc.gov/idtheft 1-877-438-4338	Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202 oag.state.md.us 1-888-743-0023	North Carolina Attorney General 9001 Mail Service Center Raleigh, NC 27699 ncdoj.gov 1-877-566-7226	Rhode Island Attorney General 150 South Main Street Providence, RI 02903 http://www.riag.ri.gov 401-274-4400
---	--	--	--

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 <http://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

Personal Information of a Minor: You can request that each of the three national credit reporting agencies perform a manual search for a minor’s Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of minor’s information to the FTC at <https://www.identitytheft.gov/>. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: <http://www.consumer.ftc.gov/articles/0040-child-identity-theft>.