LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Allen E. Sattler
650 Town Center Drive, Suite 1400
Costa Mesa, CA 92626
Allen.Sattler@lewisbrisbois.com
Direct: 714.668.5572

December 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 A2Z Field Services, LLC ("A2Z") a company that provides inspection and preservation services located in Plain City, Ohio, with regard to a recent data security incident described in greater detail below. This letter is being sent on behalf of A2Z 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 August 14, 2020, A2Z discovered that it was the victim of a sophisticated cyber-attack. Immediately after discovering the incident, A2Z hired an independent IT expert to help them investigate what happened and whether any individuals' personal information may have been accessed or acquired without authorization. After a comprehensive forensic investigation followed by extensive efforts to locate contact information of affected individuals, on December 9, 2020, A2Z determined that certain personal information may have been affected by the incident. The information that may have been accessed included Social Security numbers, drivers' license numbers, and financial account information without means to access the financial account. A2Z is not aware of any misuse of this data.

2. Number of New Hampshire residents affected.

Approximately eight (8) residents of New Hampshire may have been affected by this incident. A2Z will be notifying the potentially affected New Hampshire residents on or about December 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.

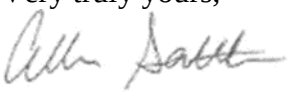
A2Z implemented additional safeguards to improve data security on their web server infrastructure. In addition, A2Z is offering identity theft protection services for twelve (12) months through Cyberscout to provide affected persons with complimentary credit monitoring. In addition, Cyberscout has created a call center to answer any questions from affected persons regarding the incident.

4. Contact Information.

A2Z 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 (714) 668-5572 or by e-mail at allen.sattler@lewisbrisbois.com.

Please let me know if you have any questions.

Very truly yours,



Allen E. Sattler of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Sample Notification Letter.

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

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

Re: Notification of Data Security Incident

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

We are writing on behalf of A2Z Field Services, LLC ("A2Z") to provide you with information about a recent data security incident that may have impacted your personal information. The privacy and security of your personal information is extremely important to us. We are sending you this letter to notify you of this incident and to inform you about steps you can take to help protect your personal information.

What Happened? On August 14, 2020, A2Z discovered that we were the victim of a sophisticated cyber-attack. Immediately after discovering the incident, we hired an independent IT expert to help us investigate what happened and whether any individuals' personal information may have been accessed or acquired without authorization. After a comprehensive forensic investigation followed by efforts to locate contact information of affected individuals, on December 9, 2020, A2Z determined that your personal information may have been affected by the incident. While we are unaware of the misuse of any information involved with this incident, we are writing to inform you about the incident and to provide you with complimentary credit monitoring services.

What Information Was Involved? Based on our investigation, the following information may have been accessed as a result of the incident: name, <<insert variable text>>.

What We Are Doing. As soon as we discovered the incident, we took the steps discussed above. We also consulted with IT experts and took the recommended steps to enhance the security of our environment in order to help prevent a similar incident from occurring in the future. Finally, out of an abundance of caution, we are offering you twelve (12) months of identity theft protection services provided by CyberScout, a company specializing in fraud assistance and remediation services.

CyberScout representatives are available for 90 days from the date of this letter to assist you with questions regarding this incident, between the hours of 8:00 am to 5:00 pm Eastern time, Monday through Friday. Please call the CyberScout help line 1-800-405-6108 and supply the fraud specialist with your unique code listed below. To extend these services, enrollment in the monitoring services described below is required.

We are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score/Cyber Monitoring**[1] services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your Experian credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud.

How do I enroll for the free services? To enroll in Credit Monitoring* services at no charge, please log on to **https://www.myidmanager.com** and follow the instructions provided. When prompted please provide the following unique code to receive services: **<CODE HERE>.** In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

What You Can Do. We recommend that you review the guidance included with this letter about how to protect your personal information and remain vigilant by reviewing account statements and monitoring free credit reports.

For More Information. If you have questions or need assistance, please call 1-800-405-6108, Monday through Friday from 8 a.m. to 5:00 p.m. Eastern time. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Amie Sparks
President/CEO
A2Z Field Services, LLC

[1] Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

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. 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