CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

ERNEST KOSCHINEG
ekoschineg@c-wlaw.com

JASON MICHAEL GOODWIN
jgoodwin@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

Telephone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

September 7, 2021

Via First Class Mail
Office of Attorney General
33 Capitol Street
Concord, New Hampshire 03302

RE: Data Breach Notification

To Whom It May Concern:

I serve as counsel for A/Z Corp. ("A/Z") and provide this notification to you of a recent data security incident. By providing this notice, A/Z does not waive any rights or defenses under New Hampshire law, including the data breach notification statute.

On July 14, 2021, A/Z became aware of a potential cyber incident involving A/Z corporate servers. A/Z immediately began working with I.T. staff and third-party computer specialists to conduct an investigation to determine how this incident occurred. As a result of a thorough investigation, A/Z discovered that limited data may have been accessed by the unauthorized actors. Upon discovery, A/Z performed an extensive review to determine whether the impacted data contained any sensitive information. A/Z has recently discovered that the impacted data contains sensitive information related to A/Z employees and has identified twenty-three (23) individuals as residents of New Hampshire. While A/Z's investigation remains ongoing, the type of information believed to be impacted includes individuals' name in combination with one or more of the following elements: date of birth, Social Security number, driver's license numbers, personal financial account number, payment card number, taxpayer id number, medical information, or health information.

A/Z is notifying the affected individuals on September 7, 2021, and is providing one (1) year of complimentary credit monitoring and identity protection services. A copy of the notification letter is attached. A/Z is also reviewing its policies and procedures related to data security. Should A/Z identify that additional New Hampshire residents were impacted as a result of this incident, A/Z will provide supplemental notification.

Please contact me should you have any questions.

Very truly yours,

CIPRIANI & WERNER, P.C.

By: _____
Ernest Koschineg

A/Z CORP
a CIANBRO company

46 Norwich Westerly Road
North Stonington, CT 06359
a-zcorp.com | 800.400.2420

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

This notice is to inform you of an incident experienced by A/Z Corp that may have involved your personal information described below. We take the privacy and security of all information very seriously. While we have no evidence of misuse of information as a result of this incident, we are providing you with information about steps you can take to help protect your information, as well as offering you complimentary identity monitoring services through Kroll.

What Happened: On July 14, 2021, we became aware of a potential cyber incident involving our corporate servers. We immediately deployed all available resources to respond to the incident, began working with independent specialists in data forensics to secure our systems to prevent any additional breach or action, and initiated an investigation to determine how this incident occurred. As a result of a thorough investigation, we discovered that limited data may have been accessed by the unauthorized actors. Upon discovery, we performed an internal review to determine whether the impacted data contained any sensitive information. While our review remains ongoing, we did determine that the information described below was present within the impacted files and are providing you with this notification.

What Information Was Involved: Personal information contained in the affected files and data may have included your name in combination with one or more of the following data elements: date of birth, Social Security number, driver's license numbers, personal financial account number, payment card number, taxpayer id number, medical information, or health information.

What We Are Doing: Upon learning of this incident, we immediately took steps to secure our systems and engage third-party forensic specialists to investigate and assist in implementing additional security measures to protect against and prevent additional security breaches. Additionally, we are notifying potentially impacted individuals and offering complimentary identity monitoring services for 12 months.

What You Can Do: We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. You may also activate the complimentary identity monitoring services we are making available to you. Due to privacy laws, we cannot register you directly. Additional information regarding how to activate the complimentary services is enclosed in the attached "Steps You Can Take to Help Protect Your Information."

For More Information: Should you have questions or concerns regarding this matter, please contact our dedicated assistance line at 1-XXX-XXX-XXXX, Monday through Friday between 8:00 am to 5:30 pm Central Time.

The security of information is of the utmost importance to us, and we will continue to take steps to protect information in our care.

Sincerely,

David Rowbotham
Director of Risk Management

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Complimentary Identity Monitoring

Activate Identity Monitoring Services

Visit **https://enroll.idheadquarters.com**[1] to activate and take advantage of your identity monitoring services.

You have until **December 8, 2021** to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

You can sign up for the identity monitoring service anytime between now and **December 8, 2021**. Due to privacy laws, we cannot register you directly. Activating this service will not affect your credit score.

Monitor Your Accounts

Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.).
2. Social Security number.
3. Date of birth.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit 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.

4. Address for the prior two to five years.
5. Proof of current address, such as a current utility or telephone bill.
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 133 Rhode Island residents affected by this incident.