8101 East Prentice Avenue, Suite 350
Greenwood Village, CO 80111 UNITED STATES

ALVARIA

VIA OVERNIGHT MAIL

Attorney General John M. Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Security Incident

To Whom it May Concern:

I am writing on behalf of Alvaria, Inc. ("Alvaria" or "the Company") to inform you that notice is being sent to New Hampshire residents regarding a data incident in which Alvaria was the victim of a cyberattack that could have resulted in certain personal information being accessed without authorization.

I. Nature of the Security Incident

On November 25, 2022, Alvaria discovered suspicious activity in one segment of its internal Corporate network. Before we could fully identify and contain the criminal actors (i.e., the Hive Ransomware group) throughout the entire Corporate network, the criminal actors executed a limited ransomware attack on November 28, 2022. We immediately investigated the incident, took steps to contain the attack, remediated our systems, and notified the Federal Bureau of Investigation. While Alvaria was still investigating the potential exfiltration of any data, on December 21, 2022, we learned that the criminal actors released corporate records on their Dark Web site. We confirmed that the data released on the Dark Web site did not include data from residents in your state. However, with the assistance of a third-party forensics company, we learned that the criminals had access to certain folders on corporate servers that contained employment-related files. Our forensics investigation could not conclusively determine whether these specific employment-related files were accessed or acquired. At present, we are unaware of any misuse of that information. Additionally, on January 26, 2023, the U.S. Department of Justice announced a coordinated law enforcement operation that dismantled the Hive Ransomware network and seized their infrastructure. Law enforcement has not indicated whether these employment-related files had been acquired.

II. Number of Residents Affected and Notified

The affected folders contain the employment-related data of 149 New Hampshire residents. The employment-related data may include an individuals'

Notices to New Hampshire residents were sent via first class mail on February 22, 2023.

III. Steps Alvaria has Taken to Address the Incident

To help protect against a similar attack in the future, we have implemented additional measures and controls to enhance our security and to aggressively monitor our environment. This includes deploying Sophos' MDR across Alvaria's systems and increasing password requirements and required password changes. We have also arranged to help protect potentially affected individuals from identity theft by offering, free of charge, 24 months of credit monitoring, dark web monitoring, and fraud remediation services through Allstate Identity Protection.

Please contact me if you have any questions.

Sincerely,

Christie Babalis
SVP, General Counsel

Alvaria Inc
c/o Cyberscout
P.O. Box 3923
Syracuse, NY 13220

8101 East Prentice Avenue, Suite 350
Greenwood Village, CO 80111 UNITED STATES

[redacted]

February 22, 2023

Re: Notice of Data Incident

Dear [redacted]:

We write to inform you about a data incident experienced by Alvaria, Inc. ("Alvaria" or "the Company") that involved some of your personal information related to your employment with the Company. We are providing you with information about the incident and steps you can take to protect yourself, should you feel it necessary to do so.

What Happened? On November 28, 2022, the [redacted] group executed a ransomware attack on a limited portion of our internal Corporate network. We immediately investigated the incident, took steps to contain the attack, remediated our systems, and notified the Federal Bureau of Investigation. While Alvaria was still investigating the potential exfiltration of any data, on December 21, 2022, we learned that the criminal actors released corporate records on their Dark Web site. We confirmed that the data released on the Dark Web site did not include your personal data. With the assistance of a third-party forensics company, we learned that the criminals had access to certain folders on corporate servers that contained employment-related files. Our forensics investigation could not conclusively determine whether these specific employment-related files were accessed or acquired. [redacted]. Law enforcement has not indicated whether these employment-related files had been acquired. Although we have no evidence of actual or attempted misuse of information contained within these employment-related files, we are providing you this notice.

What Information Was Involved? Based on our investigation, we have determined that the criminal actors may have had access to employment-related data, which may include your

What We are Doing. Upon discovery of this incident, we secured our network, implemented measures to further improve the security of our systems, safely remediated our systems and operations, and initiated an investigation into the incident. We also are notifying you so that you may take further steps to protect your information, should you feel it appropriate to do so. In addition, as part of your employment, you already are provided with access to credit monitoring, dark web monitoring, and fraud remediation services through Allstate Identity Protection at no charge to you.

What You Can Do. Please review the enclosed "*Steps You can take to Help Protect Your Information*," which describes your access to the Allstate Identity Protection service, and provides further details on how to protect yourself. We encourage you to remain vigilant against the potential for identity theft and fraud by monitoring your account statements and credit reports for any potentially suspicious activity.

More Information. We sincerely regret any inconvenience this incident may cause you. If you have additional questions, you may call our dedicated assistance line at Monday - Friday, 8:00 a.m. to 8:00 p.m. Eastern Time, excluding holidays. Representatives are available for 90 days.

Sincerely,

Christie Babalis
SVP, General Counsel

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Access to Complimentary Identity Monitoring Services

You are already covered with Allstate Identity Protection. With your coverage, you can contact Allstate Identity Protection **immediately** regarding any fraud issues, and have access to the following features:

- **Identity Monitoring**
- **Credit Monitoring**
- **Dark Web Monitoring**
- **Financial Transaction Monitoring**
- **Full Service 24/7 Fraud Remediation**
- **Up to $1 Million Identity Theft Insurance** (provides coverage for certain costs and unauthorized electronic fund transfers).

You can login to your account through your individual AIP portal. If you have never logged in, forgot the website to your individual AIP portal, or have *any questions* about the product, please contact Allstate Identity Protection's customer care team at

Free Credit Report

Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus (Equifax, Experian, and TransUnion). Obtaining a copy of your credit report from each agency on an annual basis, and reviewing it for suspicious activity, can help you spot problems and address them quickly. You can request your free credit report online at www.annualcreditreport.com or by phone at 8. You can also request your free credit report by completing the request form at: www.annualcreditreport.com, and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

Fraud Alert

As a precaution against identity theft, you can consider placing a fraud alert on your credit file. A "fraud alert" tells creditors to contact you before opening a new account or changing an existing account. A fraud alert also lets your creditors know to watch for unusual or suspicious activity. To place a fraud alert, call any one of the three major credit reporting agencies listed below. An initial fraud alert remains effective for ninety days and is free of charge. If you wish, you can renew the fraud alert at the expiration of this initial period. As soon as one credit agency confirms your fraud alert, the others are notified to place fraud alerts on your file.

Equifax®
P.O. Box 105069
Atlanta, GA 30348-5069
1-800-685-1111
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts

Experian
P.O. Box 9701
Allen, TX 75013-9701
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion®
P.O. Box 2000
Chester, PA 19016-1000
1-800-680-7289
https://www.transunion.com/fraud-alerts

Security Freeze

Under the law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of suspected identity theft, we recommend that you file a police report and obtain a copy of it.

Federal law also allows consumers to place, lift or remove a security freeze on their credit reports at no charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. Be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services.

To place a security freeze on your credit report, you must send a written request by regular, certified, or overnight mail at the addresses below to *each* of the three major credit reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com). You may also request the security freeze through *each* of the credit reporting agencies' websites or over the phone:

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-298-0045
https://www.equifax.com/personal/help/place-lift-remove-security-freeze/

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft; and
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Additional Information

You may obtain additional information about identity theft (including, a security freeze) by contacting the above, the Federal Trade Commission (FTC), or your state Attorney General, or the Federal Trade Commission (FTC). The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

For District of Columbia residents, the Attorney General may be contacted at: 400 6th Street NW, Washington, DC 20001; 202-727-3400; or oag@dc.gov.

For Kentucky residents, the Office of the Attorney General of Kentucky can be contacted at, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601; 502-696-5300; or www.ag ky.gov.

For Maryland residents, the Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 410-528-8662; or www.oag.state md.us.

For New York residents, more information about steps to take to avoid identify theft can be obtained by contacting the New York State Attorney General (https://ag.ny.gov/internet/data-breach; 1-800-788-9898), the New York State Department of State's Division of Consumer Protection (https://dos.ny.gov/consumer-protection; 1-800-697-1220), or the New York State Division of State Police (1-800-342-3619; https://www.ny.gov/agencies/division-state-police).

For North Carolina residents, the Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6400; or www ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For Oregon residents, the Attorney General may be contacted to report suspected identity theft at 1162 Court St. NE, Salem, OR 97301; 503-378-4400; or www.doj.state.or.us.

For South Carolina residents, you may also contact the South Carolina Department of Consumer Affairs at 1-800-922-1594 for guidance on avoiding and dealing with the effects of identity theft.