



150 N. Riverside Plaza, Suite 3000, Chicago, IL 60606 • (312) 819-1900

April 15, 2024

**VIA E-MAIL (ATTORNEYGENERAL@DOJ.NH.GOV)**

The Honorable John Formella  
Attorney General of the State of New Hampshire  
Office of the Attorney General  
33 Capitol Street  
Concord, New Hampshire 03301

**Re: *Preliminary Notification of Data Security Incident***

Dear Attorney General Formella:

We represent United Seating and Mobility, L.L.C., d/b/a Numotion (“Numotion”), 155 Franklin Road, Ste. 300 Brentwood, TN 37027, in connection with an incident that may have involved the personal information of eight (8) New Hampshire residents. Numotion is reporting the incident pursuant to N.H. REV. STAT. ANN. § 359-C:20. This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to this submission. While Numotion is notifying you of this incident, Numotion does not waive any rights or defenses relating to the incident, this notice, or the applicability of New Hampshire law on personal jurisdiction.

**NATURE OF THE INCIDENT**

On March 2, 2024, Numotion discovered encryption on certain network systems. Numotion immediately and proactively isolated its network, moved systems offline, and disabled user access. A few systems were encrypted during the incident, but Numotion largely prevented the spread of the malicious activity through its quick containment efforts. Numotion, through counsel, engaged a third-party forensic firm to assist with the investigation and confirm the security of Numotion’s network. The investigation determined that an unknown, third-party accessed certain systems on the Numotion network and acquired certain files from a shared file server. Numotion is in the process of reviewing the acquired files and identifying individuals whose personal information was involved.

Numotion’s review is still ongoing, however, on or around March 4, 2024, Numotion determined that certain files could have contained

of eight (8) New Hampshire residents. At this time, there is no indication that the personal information involved in this incident has been misused for the purpose of committing fraud or identity theft.

### **NOTICE TO THE RESIDENTS**

Numotion is mailing notification letters to individuals via USPS today, April 15, 2024. The notification letter includes information on protecting against potential fraud and identity theft and a toll-free telephone number to call with questions regarding the incident. For individuals whose Social Security number could have been included in the acquired files, the letter also includes an offer of complimentary credit monitoring services. Enclosed is a sample of the notice sent to the New Hampshire Residents.

### **STEPS TAKEN RELATING TO THE INCIDENT**

Upon discovery, Numotion promptly contained the incident to prevent further unauthorized access, began an internal investigation, and engaged a cybersecurity firm to assist with the investigation and confirm the security of its network. Numotion is also undertaking efforts to further reduce the risk of this type of incident from occurring in the future.

### **CONTACT INFORMATION**

Please contact me if you have any questions or if I can provide you with any further information concerning this matter.

Sincerely,

Michael J. Waters

Enclosure



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

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country>>

RE: NOTICE OF DATA BREACH

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>:

Numotion values and respects the privacy of your information, which is why we are writing to advise you of a recent incident that may have involved some of your personal information. This letter explains the incident, the steps we have taken in response, and provides information on steps you may take to help protect your information, should you feel it is appropriate to do so.

**What Happened?** On March 2, 2024, we discovered that we were the victim of a cyber-attack. Upon learning of the incident, we promptly began an investigation and worked to secure our systems. We also engaged a forensic security firm to assist with our investigation and confirm the security of our computer systems. The forensic investigation determined that an unknown, unauthorized third party accessed our computer systems between February 29, 2024, and March 2, 2024, and encrypted some of our computer files. The investigation also determined that the third party may have accessed and acquired certain files from our systems during this period.

**What Information Was Involved?** We reviewed the contents of the potentially acquired files to determine if they contained any personal information. On March 4, 2024, we determined that the files contained personal information that may have included your

**What We Are Doing.** In addition to the actions described above, we have also taken steps to reduce the risk of this type of incident occurring in the future, including enhancing our technical security measures. We are also notifying you of the incident so that you can be aware and take steps to protect your information, if you feel it is appropriate to do so. Finally, although we are not aware of any instances of fraud or identity theft resulting from this incident, out of an abundance of caution, we are offering a complimentary one-year membership of Experian IdentityWorks<sup>SM</sup> Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on prompt identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. **For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary, membership, please see the additional information attached to this letter.**

**What You Can Do.** While we have no evidence that your personal information has been misused, we encourage you to take advantage of the complimentary credit monitoring included in this letter. You can also find more information on steps to protect yourself against possible identity theft or fraud in the enclosed *Additional Important Information* page.

**For More Information.** We value the trust you place in us to protect your privacy, take our responsibility to safeguard personal information seriously, and apologize for any inconvenience this incident might cause. For further information and assistance, please call 866-528-8846 from 8:00 AM to 5:30 PM Central Time, Monday through Friday, excluding major U.S. holidays.

Sincerely,

Elizabeth Henry, Chief Human Resources Officer

## ACTIVATING YOUR COMPLIMENTARY CREDIT MONITORING

To help protect your identity, we are offering a **complimentary** membership of Experian IdentityWorks<sup>SM</sup> Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

### Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: <<b2b\_text\_6 (activation date)>> (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the **Activation Code**: <<Activation Code s\_n>>

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number <<b2b\_text\_1 (Engagement Number)>> as proof of eligibility for the identity restoration services by Experian.

### ADDITIONAL DETAILS REGARDING YOUR EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.\*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE<sup>TM</sup>:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance<sup>\*\*</sup>:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at <https://www.experianidworks.com/3bcredit> or call 877-288-8057 to register with the activation code above.

**What you can do to protect your information:** There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration) for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

\* Offline members will be eligible to call for additional reports quarterly after enrolling.

\*\* The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

### Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring 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 incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

**Credit Reports:** By law, you may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies. The three national credit reporting agencies have also agreed to provide free weekly online credit reports. You can obtain your free credit report by visiting [www.annualcreditreport.com](http://www.annualcreditreport.com), by calling toll-free 1-877-322-8228, 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 a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>. Alternatively, you may elect to purchase a copy of your credit report by contacting the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-888-4213
<a href="http://www.equifax.com">www.equifax.com</a>	<a href="http://www.experian.com">www.experian.com</a>	<a href="http://www.transunion.com">www.transunion.com</a>
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

**Fraud Alerts:** By law, you have the right to place a fraud alert on your credit report if you believe you have been, or are about to become, a victim of fraud or related crime. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at [www.annualcreditreport.com/protectYourIdentity.action](http://www.annualcreditreport.com/protectYourIdentity.action).

**Credit and Security Freezes:** By law, you have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-888-298-0045	1-888-397-3742	1-888-909-8872
<a href="https://www.equifax.com/personal/credit-report-services/credit-freeze/">https://www.equifax.com/personal/credit-report-services/credit-freeze/</a>	<a href="https://www.experian.com/freeze/center.html">https://www.experian.com/freeze/center.html</a>	<a href="https://www.transunion.com/credit-freeze">https://www.transunion.com/credit-freeze</a>
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

This notification was not delayed by law enforcement.

**Iowa Residents:** Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

**Maryland Residents:** Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, <http://www.marylandattorneygeneral.gov/>.

**New Mexico Residents:** Individuals have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting [https://files.consumerfinance.gov/f/documents/bcftp\\_consumer-rights-summary\\_2018-09.pdf](https://files.consumerfinance.gov/f/documents/bcftp_consumer-rights-summary_2018-09.pdf), or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

**New York State Residents:** New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; <https://ag.ny.gov/consumer-frauds/identity-theft>; (800) 771-7755.

**North Carolina Residents:** North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; [www.ncdoj.gov](http://www.ncdoj.gov).

**Oregon Residents:** Oregon residents are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. Oregon residents can contact the Oregon Attorney General at 1162 Court St. NE, Salem, OR 97301-4096; 503-378-4400; <https://www.doj.state.or.us/>.

**Rhode Island Residents:** [We believe that this incident affected \\_\\_\\_ Rhode Island residents.](#) Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, [www.riag.ri.gov](http://www.riag.ri.gov). You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

**Vermont Residents:** If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).