

## EXHIBIT A

PO Box 5012  
Branchburg, NJ 08876  
<FIRST> <LAST>  
<ADDRESS2>  
<ADDRESS>  
<CITY>, <State> <Zip>

Dear <First> <Last>

### NOTICE OF DATA SECURITY INCIDENT

United Language Group, LLC ("ULC" or "we") is an external third-party vendor writing on behalf of UnitedHealthcare and UnitedHealthcare Global (together, "UnitedHealthcare" or "UHC") to inform you of a data security incident that may have involved certain information about you.

ULC is not owned by or affiliated with UHC in any way: we provide language translation services to UHC, including the translation of healthcare documents such as claims, billing, and other member or provider communications. The information involved in this incident was provided to ULC in connection with those services. At this time, we have no evidence that any of the information has been misused by a third party, but we are notifying you in an abundance of caution.

We take the privacy and security of personal information seriously and sincerely regret any concern or inconvenience this incident may cause.

#### What Happened

On July 9, 2025, ULC detected suspicious activity involving certain systems within its network. Upon discovery of this incident, we promptly took steps to secure our environment and engaged independent cybersecurity professionals to investigate the nature and scope of the incident. As a result of the investigation, ULC learned that an unauthorized actor may have accessed certain information stored within its network between July 8 and July 9, 2025.

Next, we conducted a time-consuming and detailed reconstruction and analysis of the data to understand whose information was affected.

On June 19, 2026, following their own extensive review and verification of the data we provided, UHC confirmed that you were impacted by this incident.

#### What Information Was Involved

The information involved may have included your:

- Personal and contact information (such as name, address, email address, telephone number, and date of birth)
- Health insurance information
- Health and clinical information (such as diagnosis, treatment, prescription, provider, and related healthcare information)
- Government-issued identification information (such as driver's license, passport, military identification, or residence permit information)
- Financial account information (in limited instances)

#### What We Are Doing

In response to this incident, we took immediate steps to secure our systems and conducted a comprehensive investigation. We engaged a specialized third-party vendor to conduct a comprehensive review of the affected data, deployed additional monitoring tools, and will continue to enhance the security of our systems.

As an added precaution, we are offering you 24 months of credit monitoring and identity protection services at no cost to you. If you wish to activate these services, please follow the instructions included in the "Steps You Can Take to Help Protect Personal Information" section on the next page of this letter. Please note you must enroll in these services directly, as we are unable to do so on your behalf.

#### What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and errors. Additional information and resources may be found in the "Steps You Can Take to Help Protect Personal Information" section on the next page of this letter.

#### For More Information

If you have additional questions regarding this incident, please call our dedicated call center at 800729-8946, which is available between Monday - Friday 8 a.m. to 11 p.m. and Saturday 9 a.m. to 6 p.m. Eastern time. Thank you, and we look forward to assisting you.

Sincerely,

United Language Group, LLC

#### Steps You Can Take to Help Protect Personal Information

1. Credit Monitoring Enrollment. To help protect you from fraud or identity theft, we are offering you a complimentary 24-month membership to <Product>, a credit and identity-theft monitoring service. To register, please:

- Ensure that you enroll by: <Date> (Your code will not work after this date.)
- Visit the <Product> website to enroll:
- Provide your activation code: <Activation Code>

2. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

3. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting  
1-866-349-5191  
P.O. Box 105069  
Atlanta, CA 30348-5069  
[www.equifax.com](http://www.equifax.com)

Experian Fraud Reporting  
1-888-397-3742  
P.O. Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)

TransUnion Fraud Reporting  
1-800-680-7289  
P.O. Box 2000  
Chester, PA 19022-2000  
[www.transunion.com](http://www.transunion.com)

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well.

You will receive confirmation letters in the mail and will then be able to order all three credit reports. free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

4. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

5. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

0000015

California Residents: Visit the California Office of Privacy Protection ([www.oag.ca.gov/privacy](http://www.oag.ca.gov/privacy)) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, [www.ag.ky.gov](http://www.ag.ky.gov). Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, [www.oag.state.md.us/Consumer](http://www.oag.state.md.us/Consumer). Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504-cfpb-summary-your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504-cfpb-summary-your-rights-under-fcra.pdf), or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001. [www.ncdoj.gov](http://www.ncdoj.gov), Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, [www.doj.state.or.us/](http://www.doj.state.or.us/). Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General. 150 South Main Street, Providence. Rhode Island 02903. [www.riag.ri.gov](http://www.riag.ri.gov). Telephone: 401-274-4400. A total of one Rhode Island resident was notified of this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission. 600 Pennsylvania Avenue, NW Washington, DC 20580, [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft). 1-877-IDTHEFT (438-4338). TTY: 1-866653-4261.