United of Omaha Life Insurance Company
A Mutual of Omaha Company

3300 Mutual of Omaha Plaza
Omaha, NE 68175
mutualofomaha.com

[DATE]

[First_Name] [Last_Name]
[Address_Line_1]
[Address_Line_2]
[City], [State] [Zip]

Notice of Data Breach

Dear [First_Name] [Last_Name],

You are receiving this letter because United of Omaha Life Insurance Company ("United of Omaha") issued a group insurance policy to your employer, or your employer inquired about a United of Omaha group insurance policy (or you are a spouse or dependent under such policy). We are writing to inform you of an incident that involved some of your personal information. The details of the incident and steps you can take are described below.

What Happened
On April 23, 2024, United of Omaha detected unusual activity in one employee's email account and observed access by an unauthorized party. The access was the result of a phishing campaign targeting United of Omaha employees. We immediately began an investigation and hired an outside forensic computer expert to determine the size and scope of the incident. The investigation determined that the unauthorized third party had access to the employee email account between April 21, 2024 and April 23, 2024. Following a thorough review of the email account, on June 28, 2024 United of Omaha discovered that the unauthorized party may have accessed sensitive information. The attack did not compromise the security of any other systems or networks and did not affect United of Omaha's ability to conduct business.

What Information Was Involved
United of Omaha's investigation confirmed that no information in the compromised account was emailed out of the account by the unauthorized party. However, the unauthorized party may have been able to view emails or attachments related to United of Omaha's employer group insurance products. Our investigation indicates that some of your information was contained in the compromised email account. We cannot confirm exactly what data was accessed for each individual, but information that may have been accessed includes full name, demographic information (such as address and date of birth), driver's license number, health insurance policy number, social security number, employment information, and limited health information.

What We Are Doing
Upon learning of the incident, United of Omaha took a number of steps to prevent similar incidents from occurring in the future including changing the employee's Microsoft account passwords to prevent further access to the email account, hiring independent and industry-leading cybersecurity and data analysis experts to assist in the investigation, reporting the fraudulent domain associated with the attack, and re-training all employees on how to identify and report phishing campaigns.

What You Can Do
We sincerely regret any inconvenience or concern caused by this incident. As a result of this incident, we are sending you this Notice in accordance with applicable laws and regulations. To help detect and protect against

possible misuse of personal information, we recommend taking the precautionary measures described below. As a safeguard, we have arranged for Experian to provide you identity protection services for 24 months at no cost to you. The following identity protection services start on the date of this notice for use at any time during the next 24 months.

To help protect your identity, we are offering complimentary access to Experian IdentityWorks^{SM} for 24 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24 months membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** [ENROLLMENT END DATE] (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [ENROLLMENT URL]
- ***Provide your activation code: [activation code]***

ADDITIONAL DETAILS REGARDING YOUR 24 MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

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

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 files for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms and bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE^{TM}:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.
- **Lost Wallet:** Provides assistance with canceling/replacing lost or stolen credit, debit, and medical cards.
- **Child Monitoring:** For 10 children up to 18 years old, Internet Surveillance and monitoring to determine whether enrolled minors in your household have an Experian credit report are available. Also included are Identity Restoration and up to $1M Identity Theft Insurance**.

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [TOLL FREE NUMBER] by [ENROLLMENT END DATE]. Be prepared to ***provide your activation code [activation code]*** and you may be asked for your engagement number [ENGAGEMENT NUMBER] as proof of eligibility for the Identity Restoration services by Experian.

For More Information
For more information about preventing identity theft and protecting yourself against fraud, please see the attached materials.

We understand that you may have questions about this incident that are not addressed in this letter. We have established a confidential, toll-free hotline with a third party call center that is staffed with professionals familiar with this incident who can assist you with questions and steps you can take to protect against identity theft and fraud. The hotline is available at [TOLL FREE NUMBER], Monday through Saturday, from 8am – 8pm Central Standard Time. You may also visit our website at www.MutualofOmaha.com/facts.

The privacy and security of sensitive personal information is of critical importance to us, and we apologize for any inconvenience or concern because of this incident.

Sincerely,

Chief Privacy Officer
United of Omaha
3300 Mutual of Omaha Plaza
Omaha, NE 68175

* 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.

Consumer Reference Guide

As a precautionary measure, consumers may wish to regularly review account statements and periodically obtain credit reports from one or more of the national credit reporting companies. Consumers may obtain a free copy of credit reports online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. Consumers may also purchase copies of credit reports by contacting one or more of the three national credit reporting agencies using the contact information listed below.

Consumers may wish to review credit reports carefully and look for accounts or creditor inquiries that are not initiated or recognized by consumer. If anything is seen that is not understandable, including inaccuracies in home address or Social Security number, consumers should call the credit reporting agency at the telephone number on the report.

Consumers should remain vigilant for incidents of fraud and credit activity with respect to reviewing account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper authorities, including local law enforcement, the state's attorney general and/or the Federal Trade Commission ("FTC"). The FTC or a state's regulatory authority may be contacted to obtain additional information about avoiding identity theft using the contact information listed below.

Consumers may wish to regularly review explanation of benefits statements received from insurers. If medical services appearing were not received or are not receiving your benefit statements, contact the insurer at the number on the statement. Check your credit reports for any medical bills not recognized and report anything suspicious to the credit reporting agency at the phone number on the report.

Fraud Alerts: There are also two types of fraud alerts that can be placed on credit reports to put creditors on notice that a consumer may be a victim of fraud: an initial alert and an extended alert. Consumers may ask that an initial fraud alert be placed on their credit report if they suspect they have been, or are about to be, a victim of identity theft. An initial fraud alert stays on credit reports for at least one year. An extended alert may be placed on credit reports if consumers have already been a victim of identity theft, with the appropriate documentary proof, and stays on credit reports for seven years. Consumers may place a fraud alert on their credit reports by contacting the toll-free fraud number of any of the three national credit reporting agencies listed below.

Credit Freezes: Consumers have the right to place a credit freeze or security freeze (referred to as "credit freeze") on their consumer reports. A credit freeze is designed to prevent credit, loans and services from being approved in a consumer's name without the consumer's consent. Using a credit freeze, however, may delay ability to obtain credit. Consumers may request that a freeze be placed on credit reports by sending a request to a credit reporting agency on-line or by certified mail, overnight mail or regular stamped mail to the three national reporting agencies listed below. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report.

Unlike a fraud alert, a credit freeze must be separately placed on a consumer's credit file at each credit reporting company. More information can be obtained about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

Reference Numbers:
Consumers may also purchase a copy of their credit report by contacting one or more of the three national credit reporting agencies listed below:

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian: P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion: P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

Consumers can place a fraud alert on their credit report by contacting any of the three national credit reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-525-6285, www.equifax.com
Experian: P.O. Box 9532, Allen, TX 75013,1-888-397-3742, www.experian.com
TransUnion: P.O. Box 1000, Chester, PA 19022, 1-800-680-7289, www.transunion.com

You can place a credit freeze on your credit report by contacting any of the three national credit reporting agencies listed below.

Equifax: P.O. Box 105788, Atlanta, GA 30348-5788,1-800-685-1111, www.equifax.com/personal/credit-report-services
Experian: P.O. Box 9554, Allen, TX 75013, 1-888-397-3742, www.experian.com/help

TransUnion: P.O. Box 2000, Chester, PA, 19022-2000, 1-800-909-8872, freeze.transunion.com/credit-help

Federal Trade Commission: Consumers may also obtain information about preventing and avoiding identity theft from the Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For residents of Maryland: Consumers may obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For residents of Massachusetts: The following information should be included when requesting a credit freeze in Massachusetts (documentation for an individual and their spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display name and current mailing address, and the date of issue (statement dates must be recent).

Consumers also have the right to obtain a police report.

For residents of New Mexico: Consumer has rights pursuant to the Fair Credit Reporting Act ("FCRA"), such as the right to be told if information in the consumer's credit file has been used against the consumer, the right to know what is in the consumer's credit file, the right to ask for consumer's credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the FCRA, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to the consumer's file is limited; the consumer must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance received based on information in the credit report; and consumer's may seek damages from violator. Consumer may have additional rights under the FCRA not summarized here. Identity theft victims and active-duty military personnel

have specific additional rights pursuant to the FCRA. We encourage consumer to review their rights pursuant to the FCRA by visiting 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 Avenue NW, Washington, DC 20580.

For residents of New York: Consumers may obtain information about preventing and avoiding identity theft from the New York Attorney General's Office, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/ or the New York Department of State Division of Consumer Protection at http://www.dos.ny.gov/consumerprotection.

For residents of North Carolina: Consumers may obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

For residents of Oregon: Consumers are advised to report any suspected identity theft to law enforcement, including the FTC and the Oregon Attorney General. For more information on security locks, you can visit the Oregon Department of Consumer and Business Services website at dfr.oregon.gov/financial/protect/Pages/stolen-identity.aspx and click "Place a credit freeze."

For residents of Rhode Island: Consumers have the ability to file or obtain a police report. Consumers may also obtain information about preventing and avoiding identity theft from the Rhode Island Attorney General's Office, Consumer Protection Division, 150 South Main Street, Providence, RI 02903, (401) 274-4400.

For residents of Washington D.C.: Consumers may obtain information about preventing and avoiding identity theft from the Washington D.C. Attorney General's Office, 441 4th Street, NW, Washington, DC 20001, 1-202-727-3400, oag.dc.gov.