Hogan Lovells US LLP
Columbia Square
555 Thirteenth Street, NW
Washington, DC 20004
T +1 202 637 5600
F +1 202 637 5910
www.hoganlovells.com

January 28, 2022

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

By Email

To Whom it May Concern,

I am writing on behalf of Unum Group ("Unum") to inform you that Unum determined on January 19, 2022, that it had experienced a security incident impacting the personal information of Maryland residents.

On November 23, 2021, Unum learned that the contents of a Unum employee's email account had been accessed by an unknown actor. With the support of leading cybersecurity consultants, an investigation was conducted, which did not identify any other email accounts or systems as involved. The investigation did reveal that on October 28, 2021, an employee unfortunately fell victim to a phishing attack, providing his credentials to an unknown party and then approving multi-factor authentication access. The investigation also determined that the email account was impermissibly accessed between October 28, 2021, and November 15, 2021. Unum has seen no indications that personal information contained within the email account has been misused.

Unum's cybersecurity vendor conducted an extensive forensic review of the affected employee's email account. On the evening of January 18, 2022, the vendor presented Unum with a report that enabled Unum to determine on January 19, 2022, that the employee's email account contained personal information of Maryland residents including name, address, date of birth, Social Security number, and policy information. As of the date of this letter, approximately 103 Maryland residents have been identified as impacted. Unum is continuing to analyze the report and the data and may provide a supplemental report to you as Unum confirms the impacted data and individuals affected.

To help prevent this type of incident from reoccurring, Unum has provided remedial training and coaching to the employee whose account was compromised. Unum is also changing the type of multi-factor authentication that was on the employee's account to reduce the risk of improper approval of multi-factor access requests. Unum is continuing to evaluate other potential enhancements to Unum's security protocols.

Unum will provide notice by mail to affected Maryland residents, and a copy of such notice is attached. In addition to providing information regarding credit reporting agencies, government resources, security freezes, fraud alerts, and other identity protection tools, Unum is offering credit monitoring and identity protection services for two years through Experian, at no cost to the impacted individuals.

Please feel free to contact me if you have any questions or require additional information.

Sincerely,

/s/

Paul Otto
paul.otto@hoganlovells.com
(202) 637-5887

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

January 28, 2022

H4601-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 US
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

NOTICE OF DATA BREACH

Dear Sample A. Sample:

Unum is writing to tell you that we recently experienced a cybersecurity incident where an unknown actor accessed the email account of a Unum employee.

What Happened? On November 23, 2021, Unum learned that the contents of a Unum employee's email account had been accessed by an unknown actor. We investigated this incident with the support of leading cybersecurity consultants. The investigation determined that the email account was impermissibly accessed between October 28, 2021 and November 15, 2021. We have no indication that your information has been misused, but we are informing you so that you may take precautionary measures.

What Information Was Involved? The information that may have been accessed includes your [Extra1].

What We Are Doing. Upon learning that the email account was accessed by an unknown actor, we promptly took measures to secure the account. In addition, we are taking steps to reduce the risk of this type of incident reoccurring. We are modifying our email login security processes and continuing to evaluate any potential enhancements to our security protocols. We also have arranged for you to obtain, at no cost to you, 24 months of credit monitoring and other services from Experian. Information regarding the package of services is included in Attachment 1 to this letter. We also want you to know about other protective actions you can take.

What You Can Do. We are not aware of any evidence indicating that your personal information has been or will be misused. However, we recommend that you remain vigilant by reviewing your account statements and monitoring your free credit reports for signs of suspicious activity. Please find additional information in Attachment 2 to this letter. As noted above, you can enroll, at no cost to you, in 24 months of credit monitoring and other services from Experian. Information about enrollment is included in Attachment 1 to this letter.

For More Information. We regret that this incident occurred. If you have questions or concerns regarding this matter, please contact (866) 892-2278, Monday through Friday between 8 a.m. to 8 p.m. Eastern Time.

Sincerely,

T Mirza

Tariq Mirza
Assistant Vice President
Customer Contact Centers

Attachment 1: Credit Monitoring and Identity Theft Services Enrollment Information

What we are doing to protect your information:
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 month 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 April 30, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/RR3Bplus
- Provide your **activation code**: **ABCDEFGHI**

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 **(888) 397-0054** by April 30, 2022. Be prepared to provide engagement number **B023389** as proof of eligibility for the Identity Restoration services by Experian.

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, Equifax and Transunion files for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & 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™:** 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**.

What You Can Do. Please review the enclosed *Information about Identity Theft Protection* for additional information on how to protect against identity theft and fraud. You may also take advantage of the complimentary identity protection services being offered.

For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call (888) 397-0054 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number B023389.

*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.

Attachment 2: Additional Information

You should be cautious about using email to provide sensitive personal information, whether sending it yourself or in response to email requests. You should also be cautious when opening attachments and clicking on links in emails. Scammers sometimes use fraudulent emails or other communications to deploy malicious software on your devices or to trick you into sharing valuable personal information, such as account numbers, Social Security numbers, or usernames and passwords. The Federal Trade Commission (FTC) has provided guidance at https://www.consumer.ftc.gov/articles/0003-phishing.

You should review your financial statements and accounts for signs of suspicious transactions and activities. If you find any indication of unauthorized accounts or transactions, you should report the possible threat to local law enforcement, your state's Attorney General's office, or the FTC. You will find contact information for some of those entities below. If you discover unauthorized charges, promptly inform the relevant payment card companies and financial institutions.

Fraud Alert Information

Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Whether or not you enroll in the credit monitoring product offered, you also have the right to place an initial fraud alert on your file at no cost. An initial fraud alert lasts 1 year and is placed on a consumer's credit file. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. Fraud Alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A Fraud Alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit.

Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies. You may also contact any of the consumer reporting agencies or the FTC for more information regarding Fraud Alerts. The contact information for the three nationwide credit reporting companies is:

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5788	Allen, TX 75013-9554	Chester, PA 19016-2000
1-888-766-0008	1-888-397-3742	1-800-680-7289

Free Credit Report Information

You have rights under the federal Fair Credit Reporting Act. These include, among others, the right to know what is in your credit file; the right to dispute incomplete or inaccurate information; and the right to ask for a credit score. Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, we recommend that you check your account statements and credit reports periodically. You should remain vigilant for incidents of fraud and identity theft. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency or state Attorney General and file a police report. Get a copy of the report; many creditors want the information it contains to alleviate you of the fraudulent debts. You also should file a complaint with the FTC using the contact information below. Your complaint will be added to the FTC's Consumer Sentinel database, where it will be accessible to law enforcement for their investigations.

You may also contact the FTC at the contact information below to learn more about identity theft and the steps you can take to protect yourself and prevent such activity. If you are a resident of the District of Columbia, Iowa, Maryland, New York, North Carolina, or Oregon, you can also reach out to your respective state's Attorney General's office at the contact information below. All other residents can find information on how to contact your state Attorney General at https://www.naag.org/ find-my-ag/.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1.877.FTC.HELP (382.4357) /
www.ftc.gov/idtheft

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301
1-877-877-9392 /
https://justice.oregon.gov

New York Attorney General's Office
The Capitol
Albany, NY 12224-0341
1-800-771-7755
https://ag.ny.gov/consumer-frauds-bureau/identity-theft

North Carolina Department of Justice
114 West Edenton Street
Raleigh, NC 27603
1-919-716-6400
https://ncdoj.gov/protecting-consumers/identity-theft/

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, DC 20001
1-202-727-3400 / oag.dc.gov

Maryland Attorney General's Office
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023 /
www.marylandattorneygeneral.gov

Consumer Protection Division
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 50319
1-515-281-5926
www.iowaattorneygeneral.gov

Security Freeze Information
You have the right to request a free Security Freeze (aka "Credit Freeze") on your credit file by contacting each of the three nationwide credit reporting companies via the channels outlined below. When a Credit Freeze is added to your credit report, third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. A Credit Freeze can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. You may also contact any of the consumer reporting agencies or the FTC for more information regarding Security Freezes.

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
http://www.equifax.com/personal/credit-report-services/credit-freeze/
1-800-349-9960

TransUnion Security Freeze
PO Box 2000
Chester, PA 19016
www.transunion.com/freeze
1-888-909-8872

Experian Security Freeze
PO Box 9554
Allen, TX 75013
www.experian.com/freeze
1-888-397-3742

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

1) Full name, with middle initial and any suffixes;
2) Social Security number;
3) Date of birth (month, day, and year);
4) Current address and previous addresses for the past five (5) years;
5) Proof of current address, such as a current utility bill or telephone bill;
6) Other personal information as required by the applicable credit reporting agency;

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

New Mexico residents: You have the right to obtain a Credit Freeze or submit a declaration of removal under the New Mexico Fair Credit Reporting and Identity Security Act. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the New Mexico Fair Credit Reporting and Identity Security Act.

Monitor Your Personal Health Information
If applicable to your situation, we recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the website of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.