



UnitedHealthcare Privacy Office
185 Asylum Street
Hartford, CT 06103

January 13, 2022

VIA ELECTRONIC MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
idtheft@oag.state.md.us

Maryland Insurance Administration
Attn: Dawna Kokosinski, Chief Market Analyst
200 St. Paul Place
Baltimore, MD 21202
dawna.kokosinski@maryland.gov

RE: Privacy Breach Notification

Dear Sir or Madam,

We are writing to inform you of a recent privacy incident that impacted twenty-four (24) Maryland residents.

On November 17, 2021, the UnitedHealthcare (“UHC”) Privacy Office was notified of a privacy incident involving our Business Associate, Medical Review Institute of America (“MRIoA”). MRIoA performs various medical reviews for our plans.¹

Upon investigation, we discovered that between November 2, 2021 and November 9, 2021, MRIoA had been the target of a cyber security incident. MRIoA detected and contained the situation on November 9; however, MRIoA confirmed that the bad actor successfully acquired protected health information from their systems. It should be noted that this incident did not directly impact UHC systems.

In response to the breach, MRIoA engaged a forensic team to conduct an analysis of the breach and to implement additional technical safeguards to bolster security. At this time, neither MRIoA nor their forensic team have found any indication that the data has been misused.

¹ It is UHC’s understanding that MRIoA submitted a notice to the Office of the Attorney General on January 6, 2022.

On or about January 17, 2022, MRIOA will mail a notification letter via United States Postal Service First-Class mail to the impacted members. A copy of the consumer notice is attached with this letter.

Although there is no evidence to suggest that the affected individuals' information has been misused in any way or that any financial account information was compromised, MRIOA is providing identity theft protection for one (1) year. Further, the notification letter recommends steps the affected individuals can take to protect their identity, including how to place a fraud alert and/or security freeze on their credit file and provides them with the contact information for the national credit reporting agencies and the Federal Trade Commission.

As you know, protecting the personal information of our consumers is paramount to us. We will be working internally to ensure additional steps are put in place to prevent such incidents from recurring.

Please let me know if you have any questions or concerns.

Yours Truly,

A handwritten signature in blue ink, appearing to read "Ben Schimelman".

Benjamin Schimelman

Associate General Counsel – Privacy, LCRA

UnitedHealthcare Corporate

O 860-702-5052 | E Benjamin_schimelman@uhc.com

Notice of Breach of Security System
To the Maryland Insurance Commissioner

This Notice of Breach form must be completed if the carrier: (i) conducts an investigation required under § 14-3504(b) or (c) of the Commercial Law Article; and (ii) determines that the breach of the security of the system creates a likelihood that personal information has been or will be misused.

Company Name: UnitedHealthcare Insurance Company

Name of person filing this Notice: Benjamin I. Schimelman Phone Number: 860-702-5052

Email Address: benjamin_schimelman@uhc.com

Provide a brief description of the circumstances of the security breach.

Please see the letter attached with this form.

In addition to the above, this Notice must be accompanied by the following documents:

- A form copy of all notifications sent to consumers as a result of the security breach.

- A copy of the notice of a breach of the security of a system submitted to the Maryland Attorney General, as required under § 14-3504(h).

MARYLAND INSURANCE ADMINISTRATION
MARKET CONDUCT ACTION
CERTIFICATE OF COMPLIANCE

Pursuant to Code of Maryland Regulations (“COMAR”) 31.04.20.05 E, I ^{Benjamin I. Schimelman}_____ hereby certify to the best of my knowledge, information, and belief, that the information hereto submitted to the Maryland Insurance Administration (“Administration”) represents a full, complete, and truthful Notice, as required under Insurance Article, § 4-406, Annotated Code of Maryland.

I further attest that I am an authorized officer/representative of the Company, that I have undertaken an adequate inquiry to provide this certification to the Commissioner, and am authorized to bind the company to the responses provided.

Signature:	<u>Users, bschimmel</u> Digitally signed by Users, bschimmel Date: 2022.01.13 13:33:52 -05'00'
Print Name:	<u>Benjamin I. Schimelman</u>
Company:	<u>UnitedHealthcare Insurance Company</u>
Title:	<u>Associate General Counsel</u>
Date:	<u>January 13, 2022</u>



<FirstName> <LastName>

<Address1>

<Address2>

<City><State><Zip>

<date>

Re: Notice of Data Breach

Dear <First Name> <Last Name>,

At the Medical Review Institute of America (“MRIoA”), a business associate of your health insurer, we value transparency and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that involved your protected health information, what we did in response, and steps you can take to protect yourself against possible misuse of the information.

What Happened

On November 9, 2021, we learned that we were the victim of a sophisticated cyber-attack. Once we found out, we quickly took steps to secure and safely restore our systems and operations. Further, we immediately engaged third-party forensic and incident response experts to conduct a thorough investigation of the incident's nature and scope and assist in the remediation efforts. We also contacted the FBI to inform them of the incident and seek guidance. On November 12, 2021, we discovered that the incident involved the unauthorized acquisition of information.

On November 16, 2021, to the best of our ability and knowledge, we retrieved and subsequently confirmed the deletion of the obtained information. Our investigation into the cause of the incident is ongoing. However, once we retrieved the information, we began determining the individuals impacted in the incident. Further, based on a comprehensive review, we discovered that your protected health information was impacted in the incident.

However, as of now, we have no evidence indicating misuse of any of your information.

What Information Was Involved

The types of protected health information potentially involved are your demographic information (i.e., first and last name, gender, home address, phone number, email address, date of birth, and social security number); clinical information (i.e., medical history/diagnosis/treatment, dates of service, lab test results, prescription information, provider name, medical account number, or anything similar in your medical file and/or record); and health insurance information (i.e., health insurance policy and group plan number, group plan provider, claim information). The obtained information did not include financial account information.

What We Are Doing

As explained above, we took immediate steps to secure our systems and engaged third-party forensic experts to assist in the investigation. Further, in response to this incident, we implemented and/or are continuing to implement additional cybersecurity safeguards to our existing robust infrastructure to better minimize the likelihood of this type of event occurring again, including:

- Constant monitoring of our systems with advanced threat hunting and detection software;
- Adding additional authentication protections when attempting to access the systems;
- New servers built from the ground up to ensure all threat remnants were removed;
- Working with external third-party cybersecurity experts to assist us in our security efforts;
- Deploying a hardened and new backup environment;
- Enhancing our employee cybersecurity training; and
- Reviewing, revising, and amending our existing cybersecurity policies as necessary.

2875 S. Decker Lake Drive Suite 300, Salt Lake City, UT 84119 / PO Box 25547 Salt Lake City, UT 84125-0547

(801) 261-3003 (800) 654-2422 FAX (801) 261-3189

www.mrioa.com A URAC, HITRUST and NCQA Accredited Company

What You Can Do

The security and privacy of the information contained within our systems is a top priority for us. Therefore, while we have no evidence indicating your information was misused, we strongly recommend that you remain vigilant, monitor and review all of your financial and account statements, and report any unusual activity to the institution that issued the record and law enforcement. In addition, please see “***OTHER IMPORTANT INFORMATION***” on the following pages for guidance on how to best protect your identity.

Also, to help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Fraud Consultation, and Identity Theft Restoration.

Visit <<**IDMonitoringURL**>> to activate and take advantage of your identity monitoring services.

*You have until <<**Date**>> to activate your identity monitoring services.*

Membership Number: <<**Member ID**>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via our automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central time, excluding major U.S. holiday. Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through our automated phone system.

Additional information describing your services is included with this letter.

For More Information

We sincerely regret this incident occurred and for any concern it may cause. We understand that you may have questions about it beyond what is covered in this letter. To assist you with questions regarding this incident, representatives are available for 90 days from the date of this letter, 8:30 am to 5:00 pm Central time, Monday through Friday, excluding major U.S. holidays. Please call the helpline 1-xxx-xxx-xxxx and supply the call center representatives with your unique code listed below. To extend these services, enrollment in the monitoring services described above is required.

Sincerely yours,

Ron Sullivan, President/CEO



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

OTHER IMPORTANT INFORMATION

Obtain and Monitor Your Credit Report. We recommend that you obtain a free copy of your credit report from each of the three nationwide credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free 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 access the request form at <https://www.annualcreditreport.com/requestReport/requestForm.action>. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. The three nationwide credit reporting agencies' contact information are provided below to request a copy of your credit report or general identified above inquiries.

Equifax (888) 766-0008 P.O. Box 740256 Atlanta, GA 30348 www.equifax.com	Experian (888) 397-3742 P.O. Box 2104 Allen, TX 75013 www.experian.com	TransUnion (800) 680-7289 P.O. Box 1000 Chester, PA 19016 www.transunion.com
---	--	--

Security Freeze (also known as a Credit Freeze). Following is general information about how to request a security freeze from the three credit reporting agencies. While we believe this information is accurate, you should contact each agency for the most accurate and up-to-date information. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please 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. In addition, in some states, the agency cannot charge you to place, lift or remove a security freeze. There might be additional information required, and as such, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided above).

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-freeze/	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 www.experian.com/freeze	TransUnion Security Freeze & Fraud Victim Assistance Dept. P.O. Box 1000 Chester, PA 19016 https://www.transunion.com/credit-freeze
---	---	--

Consider Placing a Fraud Alert on Your Credit Report. You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least twelve months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three nationwide credit reporting agencies identified above. Additional information is available at <https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

Remain Vigilant, Review Your Account Statements and Notify Law Enforcement of Suspicious Activity. As a precautionary measure, we recommend that you remain vigilant by closely reviewing your account statements and credit reports. If you detect any suspicious activity on an account, we strongly advise that you promptly notify the financial institution or company that maintains the account. Further, you should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC). To file a complaint or to contact the FTC, you can (1) send a letter to the *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580; (2) go to IdentityTheft.gov/databreach; or (3) call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, a database made available to law enforcement agencies.

Take Advantage of Additional Free Resources on Identity Theft. We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some

helpful tips on how to protect your information. Additional information is available at <https://www.consumer.ftc.gov/topics/privacy-identity-online-security>. For more information, please visit [IdentityTheft.gov](https://www.consumer.ftc.gov/articles/pdf/0009-identity-theft-a-recovery-plan.pdf) or call 1-877-ID-THEFT (877-438-4338). In addition, a copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at <https://www.consumer.ftc.gov/articles/pdf/0009-identity-theft-a-recovery-plan.pdf>.

California residents may wish to review the recommended privacy protection steps outlined in the Breach Help-Consumer Tips from the California Attorney General, which can be found at: <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/cis-17-breach-help.pdf>.

Connecticut residents may wish to review the information the Attorney General, who can be contacted at the Office of the Attorney General, Consumer Protection Department, 165 Capitol Avenue, Hartford, CT 06106, calling 1-860-808-5400 or visiting <https://portal.ct.gov/>.

District of Columbia residents: You can obtain information from the FTC and the Office of the Attorney General for the District of Columbia about steps to take to avoid identity theft. You can contact the D.C. Attorney General at: 441 4th Street, NW, Washington, DC 20001, 202-727-3400, www.oag.dc.gov.

Iowa residents may also wish to contact the Office of the Attorney general on how to avoid identity theft by calling 515-281-5164 or by mailing a letter to the Attorney General at: *Office of the Attorney General of Iowa*, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Maryland residents may wish to review the information the Attorney General, who can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, or visiting www.oag.state.md.us.

Massachusetts residents: State law advises you that you have the right to obtain a police report. Further, you have the right to obtain a security freeze on your credit report free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. To request a security freeze be placed on your credit report, please be prepared to provide any or all of the following: your full name, social security number, address(es), date of birth, a copy of a government issued identification card, a copy of a utility bill, bank or insurance information, or anything else the credit reporting agency needs to place the security freeze. Further information regarding credit freezes, including the contact information for the credit reporting agencies, may be found above in section titled "Security Freeze (also known as a Credit Freeze)."

New Hampshire residents have the right to ask that the three nationwide credit reporting agencies place fraud alerts in their file (as described above) and or request a security freeze (as described above). To place or fraud alert on your file or request the security freeze, please contact three credit reporting agencies identified above.

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.

New York residents: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: New York Attorney General's Office Bureau of Internet and Technology, (212) 416-8433, <https://ag.ny.gov/internet/resource-center> or [NYS Department of State's Division of Consumer Protection](https://www.dos.ny.gov/consumerprotection), (800) 697-1220, <https://www.dos.ny.gov/consumerprotection>.

North Carolina residents may wish to review the information provided by the North Carolina Attorney General at www.ncdoj.gov, or by contacting the Attorney General by calling 877-5-NO-SCAM (Toll-free within North Carolina) or by mailing a letter to the Attorney General at *North Carolina Attorney General's Office, Consumer Protection Division*, 9001 Mail Service Center Raleigh, NC 27699.

Oregon residents: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877- 9392, www.doj.state.or.us.

Rhode Island residents have the right to obtain a police report (if one was filed. Alternatively, you can file a police report). Further, you can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services.

West Virginia residents have the right to ask that the three nationwide credit reporting agencies place fraud alerts in their file (as described above) and or request a security freeze (as described above). To place or fraud alert on your file or request the security freeze, please contact three credit reporting agencies identified above.