21792

UnitedHealthcare Privacy Office
2720 N. Tenaya Way
NV018-S500
Las Vegas, NV 89128

Date

Name
Address Line 1
Address Line 2
City, STATE, Zip code

Dear Name,

We are writing to let you know about a privacy issue involving some of your personal information. On May 28, 2021, UnitedHealthcare (UHC) learned of an issue impacting your current or former UHC COBRA coverage. On June 30, 2021, the UHC Privacy Office learned that your name and Social Security number was visible to another individual on the uhcservices.com COBRA member portal. No additional information such as address, date of birth, medical information or financial account information was disclosed as a result of this issue.

The issue occurred on the COBRA member portal, uhcservices.com, from May 24, 2021 to June 3, 2021. During this time, your name and Social Security number was able to be viewed by another individual when they viewed their COBRA Continuation Coverage Notice in Connection with Extended Election Periods letter.

Upon discovery of the issue, we took prompt action to investigate the matter. The Social Security number information was removed from the portal. Our thorough investigation determined this issue was the result of a system error when software was updated to provide current or former COBRA members with electronic copies of recently mailed letters regarding their COBRA benefits. A temporary fix which scrubs the Social Security number information from the data is in place to ensure this information is not further disclosed on the portal. A permanent fix is in development and will be implemented once extensive testing validates the system fix.

While we have no indication that your information has been misused, as a precaution to help you detect any possible misuse of your personal information, we recommend that you regularly review your bank and credit card statements. If you notice any suspicious activity, please immediately contact your financial institution and/or credit card company. In addition, we are offering you two years of free "LifeLock® Identity Theft Protection Services," which includes proactive identity theft protection, identity theft alerts, address change verification, annual copies of your credit report from all three national credit bureaus, and comprehensive recovery services if you become a victim of identity theft during your LifeLock membership. We have enclosed instructions for registering for this service and the enclosed Reference Guide provides details about additional steps you may wish to take to monitor and protect your credit and finances.

UHC takes this matter very seriously and is committed to protecting the privacy and security of your personal information. We are reinforcing our existing policies and practices with employees and evaluating additional safeguards to help prevent a similar incident from occurring in the future.

We deeply regret any inconvenience or concern caused by this incident. If you have any questions or concerns, please call us toll free at 866-747-0048.

Sincerely,

Sandra Haase

Sandra Haase
Senior Privacy Investigator

[INSERT LIFELOCK CREDIT MONITORING SUBSCRIPTION INSTRUCTIONS]

Reference Guide

Order Your Free Credit Report

You are entitled to receive your credit report from each of the three national credit reporting agencies once per year, free of charge. You may obtain your free annual credit report from each of the national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free at 877-322-8228, or by mailing your request to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually. They provide free annual credit reports only through the website or toll-free number.

When you receive your credit report(s), review them carefully. Look for any inaccurate information and contact the appropriate credit reporting agency to notify of any incorrect information, including accounts you did not open; requests for your credit report from anyone that you did not apply for credit with; or inaccuracies regarding your personal identifying information, such as your home address and Social Security number. If you find anything that you do not understand or that is incorrect, contact the appropriate credit reporting agency using the contact information on the credit report as soon as possible so the information can be investigated, and if found to be in error, corrected.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in your financial accounts, promptly notify your credit card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission. If you believe your identity has been stolen, the U.S. Federal Trade Commission ("FTC") has created a one-stop resource site that provides and interactive checklist that walks through the steps people need to take upon learning that their identity has been stolen or their personal information has been compromised in a data breach. The FTC recommends that you take these additional 4 steps right away when you become a victim:

Step 1: Call the companies where you know fraud occurred.

Step 2: Place a fraud alert and get your credit report.

Step 3: Report identity theft to the FTC.

Step 4: File a report with your local police department.

A checklist of the steps listed above and links to forms and other helpful information can be found on the site at IdentityTheft.gov.

You can learn more about how to protect yourself from becoming a victim of identity theft by contacting the FTC at the address below or visiting the website below:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
TTY: 1-866-653-4261
http://www.consumer.ftc.gov/features/feature-0014-identity-theft

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Credit Agency	Mailing Address	Phone Number	Website
Equifax	Equifax Information Services LLC P.O. Box 105069 Atlanta, GA 30348-5069	800-525-6285	www.equifax.com
Experian	Experian P.O. Box 9554 Allen, TX 75013	888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	800-680-7289	https://fraud.transunion.com/

Place a Security Freeze on Your Credit File

You may wish to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze by contacting the credit bureaus at:

Credit Agency	Mailing Address	Phone Number	Website
Equifax	Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348	Automated line: 800-685-1111 (NY residents, please call 800-349-9960)	www.freeze.equifax.com
Experian	Experian P.O. Box 9554 Allen, TX 75013		www.experian.com
TransUnion	TransUnion Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19016	888-909-8872	https://freeze.transunion.com

The credit bureaus may charge a reasonable fee to place a freeze on your account, and may require that you provide proper identification prior to honoring your request.

For Maryland and North Carolina Residents. You can obtain information from your state's Attorney General's Office about steps you can take to help prevent identity theft.

You can contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023/TDD: 1-410-576-6372
http://www.oag.state.md.us/Consumer/index.htm

You can contact the North Carolina Attorney General at:
North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
1-919-716-6400
http://www.ncdoj.gov/Protect-Yourself/2-4-3-Protect-Your-Identity.aspx

For California Residents. You can obtain additional information from the California Department of Justice's Privacy Enforcement and Protection Unit (http://oag.ca.gov/privacy) to learn more about protection against identity theft.

Precautions to Help You Avoid Becoming a Victim

1. Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about you, your employees, your colleagues or any other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.

2. Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.

3. Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.

4. Do not send sensitive information over the Internet before checking a website's security (for more information, see Protecting Your Privacy, http://www.us-cert.gov/ncas/tips/ST04-013).

5. Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).

6. If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org).

7. Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic (for more information, see Understanding Firewalls, http://www.us-cert.gov/ncas/tips/ST04-004; Understanding Anti-Virus Software, http://www.us-cert.gov/ncas/tips/ST04-005; and Reducing Spam, http://www.us-cert.gov/ncas/tips/ST04-007).

8. Take advantage of any anti-phishing features offered by your email client and web browser.

9. Employees should take steps to monitor their personally identifiable information and report any suspected instances of identity theft to the FBI's Internet Crime Complaint Center at www.ic3.gov.