UnitedHealthcare Privacy Office
185 Asylum Street
Hartford, CT 06103

August 17, 2022

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

Submitted Via:
Idtheft@oag.state.md.us

RE: *Privacy Breach Notification*
UHC File #: 487183

Dear Office of the Attorney General:

UnitedHealthcare ("UHC" or "We") are writing to inform you of a recent data incident that affected Maryland residents. On June 22, 2022 we were notified of an incident by our business associate, WEX Health. On June 12, 2022, WEX experienced a software error which resulted in FSA/HRA claim follow-up emails being emailed to the incorrect recipients.

On June 22, 2022, we confirmed that one (1) Maryland resident was impacted as a result of the incident. The information involved may have included the individuals' first and last name, address, account ID number, employer name, claim number, flexible spending account or reimbursement plan transaction date, merchant name(s) (which at times may have reflected a provider's name), plan information and, potentially, reason for a denied charge. This incident did not involve the disclosure of the individuals Social Security number, driver's license number, or date of birth.

On August 19, 2022 written notice was provided to one Maryland resident who may be potentially affected by this incident. A copy of the template notice letter that was sent to affected individuals is enclosed.

UHC will notify other regulatory agencies as required.

We take such matters as this very seriously. There is no evidence to suggest that any affected individuals' information has been misused in anyway. Additionally, the notification letter sent to affected individuals recommends steps they can take to protect their identity, including informing them that they should report suspected incidents of identity theft to local law enforcement or the attorney general. It also explains to them 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.

Protecting the personal information of individuals is very important to us. We maintain an information security program and are working with WEX to put additional protections in place to prevent such incidents from occurring in the future, including retraining staff, reinforcing existing policies and practices, and evaluating additional safeguards.

If you have any questions about this incident, please contact me directly.

Sincerely,

Joshua Devine, CIPP/US
Investigations Lead Counsel/Associate General Counsel – Privacy & Cyber, LCRA
UnitedHealthcare Corporate

O 860-702-6805
E joshua_devine@uhc.com

185 Asylum Street | CT039-020A| Hartford, Connecticut 06103

Privacy Office
ATTN: Logan Irmscher
185 Asylum Street, CT039-020A
Hartford, CT 06103

August 19, 2022

Name
Address
Address

Dear Name,

We are writing to let you know about a privacy issue involving some of your health information. On June 22, 2022, BASE was informed that some of your health information may have been emailed to another individual in error. We believe this incident occurred on June 12, 2022, and June 13, 2022.

The information that was involved included your first and last name, address, account ID number, employer name, claim number, flexible spending account or reimbursement plan transaction date, merchant name(s) (which at times may have reflected a provider's name), plan information and, potentially, reason for a denied charge. This incident did not involve disclosure of your Social Security number, driver's license number, date of birth, or financial account information.

Upon discovery, we took prompt action to investigate the matter. It was determined that a system error with our vendor, WEX Health, caused your FSA/HRA claim follow-up letter to be emailed to another individual. The system error has been corrected. At this time, we have no evidence to support that your information has been used in a malicious manner.

If you received or viewed any e-mail notifications with a claim follow-up letter on June 12 on June 13, 2022, we request that you permanently delete the e-mail and destroy any copies of the email and letters.

We are not aware that your information was misused. As a precaution to protect against misuse of your information, we recommend that you regularly monitor account statements that you receive from us to check for any unfamiliar health care charges. If you notice any suspicious activity, please contact us at 800-309-8012. If you do not regularly receive account statements, you may request that we send you these statements following the charge of any health care services in your name or plan number by contacting the number provided above.

In addition, you may want to order copies of your credit reports from each of the three national credit reporting agencies to check for any inaccurate information. If you notice any suspicious activity, contact the credit reporting agencies using the contact information provided in the attached Reference Guide.

Privacy Office
ATTN: Logan Irmscher
185 Asylum Street, CT039-020A
Hartford, CT 06103

We suggest that you retain this notice for your records in case of any future problems with your flexible spending account or reimbursement plan.

BASE takes this matter very seriously and is committed to protecting the privacy and security of your personal health information. We deeply regret any inconvenience or concern caused by this incident. If you have any questions or concerns or would like to discuss this issue further, please do not hesitate to call me at (203) 447-4538, 9am – 3pm Eastern Time.

Cordially,

Logan Irmscher
Privacy Investigator
UnitedHealthcare Privacy Office

Privacy Office
ATTN: Logan Irmscher
185 Asylum Street, CT039-020A
Hartford, CT 06103

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 1-877-322-8228, 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/steps.

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
1-877-438-4338
1-866-653-4261 (TTY)
http://www.consumer.ftc.gov/features/feature-0014-identity-theft

Privacy Office
ATTN: Logan Irmscher
185 Asylum Street, CT039-020A
Hartford, CT 06103

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 Equifax Fraud Request Form *Mail the fraud request form to the address listed above.	1-800-525-6285	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
Experian	Experian P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289	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. 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. You can request a security freeze by contacting the credit bureaus at:

Credit Agency	Mailing Address*	Phone Number	Website
Equifax	Equifax Security Freeze	Automated line: 1-800-349-9960	https://www.equifax.com/personal/credit-report-services/credit-freeze//

Privacy Office
ATTN: Logan Irmscher
185 Asylum Street, CT039-020A
Hartford, CT 06103

	P.O. Box 105788 Atlanta, GA 30348 Equifax Freeze Request Form *Mail the freeze request form to the address listed above.	Customer Care: 1-888-298-0045	
Experian	Experian P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com/freeze
TransUnion	TransUnion P.O. Box 160 Woodlyn, PA 19016	1-888-909-8872	https://www.transunion.com/credit-freeze

Additional Attorney General Office Identity Theft Resources. You can obtain information from your state's Attorney General's Office about steps that you can take to help prevent identify theft. Please see the information below for states that provide these resources:

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

For District of Columbia Residents. You can obtain additional identity theft information from the District of Columbia's Attorney General Office (https://oag.dc.gov/consumer-protection/consumer-alert-identity-theft) to learn more about protection against identity theft.

For Maryland Residents. You can contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
25th Floor
Baltimore, MD 21202

Phone: 1-410-576-6491
Fax: 1-410-576-6566
Email: idtheft@oag.state.md.us
Website: https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx

For North Carolina Residents You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
Consumer Protection Division

Privacy Office
ATTN: Logan Irmscher
185 Asylum Street, CT039-020A
Hartford, CT 06103

9001 Mail Service Center
Raleigh, NC 27699-9001

Phone: 1-877-566-7226 (Toll-free within North Carolina), 1-919-716-6000

Website: https://ncdoj.gov/

Identity Theft Link: Protecting Your Identity - ID Theft Protection by NC DOJ.

For Oregon Residents. You can obtain additional identity theft information from the Oregon Attorney General Office (https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/identity-theft/) to learn more about protection against identity theft.

For Rhode Island Residents. You can contact the Rhode Island Attorney General at:

Rhode Island Office of the Attorney General
150 South Main Street
Providence, Rhode Island 02903

Phone: 1-401-274-4400
Fax: 1-401-462-9532
Email: DBR.Insurance@dbr.ri.gov
Website: http://www.riag.ri.gov/ConsumerProtection/About.php#

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.