UnitedHealthcare Privacy Office
185 Asylum Street
Hartford, CT 06103

May 5, 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 two (2) Maryland residents.

On April 13, 2022, the UnitedHealthcare ("UHC") Privacy Office was notified of a privacy incident involving our lockbox vendor, Wells Fargo.

Upon investigation, Wells Fargo discovered that between October 14, 2021, and January 11, 2022, a Wells Fargo employee used a personal electronic device to capture images of checks remitted by or on behalf of UHC members. Wells Fargo was notified of the issue by another customer who discovered their information online at which point Wells Fargo commenced an investigation and suspended the employee's access to the lockbox facility. Wells Fargo attributed the delay in notifying UHC of this incident to the manually intensive process of reviewing the employee's activity to determine what information was compromised. It should be noted that this incident did not directly impact UHC systems.

In response to the breach, Wells Fargo terminated the employee and has instituted a policy prohibiting the use or possession of personal electronic devices capable of capturing images within the lockbox facility. Further, Wells Fargo is planning to increase the video surveillance of the lockbox facility. Finally, Wells Fargo scanned the internet for the impacted member's information but has not found any evidence that the information was being offered for sale.

On or about May 13, 2022, UHC 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, Wells Fargo is providing identity theft protection for two (2) years. 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,

Benjamin Schimelman
Associate General Counsel – Privacy, LCRA
UnitedHealthcare Corporate
O 860-702-5052 **|** **E** Benjamin_schimelman@uhc.com

RADAR #464366

UnitedHealthcare Privacy Office
185 Asylum Street, CT039-020A
Hartford, CT 06103

May [ ], 2022

[Name]
[Street]
[City, State ZIP]

Dear [First Name],

We are writing to let you know about a privacy issue involving some of your health information. On April 13, 2022, our lockbox vendor, Wells Fargo, informed us that an employee inappropriately accessed one or more of the checks processed at a Wells Fargo facility. We believe the incident began October 14, 2021.

The information included a combination of the following: member name, member number, checking account number, and address. This incident did not involve the disclosure of your Social Security number, driver's license number, or any sensitive medical information.

We deeply regret this incident and any inconvenience or concern that it may cause. Upon discovery, we took prompt action to investigate the matter. Our investigation revealed that a Wells Fargo employee captured images of checks using a personal electronic device and may have shared those images with an unauthorized third party. In response to this incident, Wells Fargo terminated the employee and instituted a policy prohibiting the possession or use of personal electronic devices in its lockbox facility. Further, Wells Fargo plans to increase the video surveillance and review of its lockbox facility.

As a precaution, to help you detect any possible misuse of your personal information, Wells Fargo is offering you two (2) years of free "Experian IdentityWorks℠," which includes identity theft detection, credit report monitoring, internet surveillance, and resolution of identity theft. Details of your complimentary subscription are enclosed along with instructions for registering for this service.

We also recommend that you regularly monitor account statements and the explanation of benefits statements that you receive from your plan to check for any unfamiliar health care services. If you notice any health care services that you did not receive listed on an explanation of benefits statement, please contact your plan at the number on your member identification card. If you do not regularly receive explanation of benefits statements, you may request that your plan send you these statements following the provision of any health care services in your name or plan number by contacting your plan at the number on your member identification card.

The enclosed Reference Guide provides additional steps you may take to monitor and protect your credit and finances. We suggest you retain this notice for your records in case of any future problems with your medical records.

UnitedHealthcare takes this matter very seriously and is committed to protecting the privacy and security of our members' health information. We deeply regret any inconvenience or concern caused by this incident. If you have any questions or concerns, please call me toll free at 800-328-5979, TTY 711, or direct at 860-702-5052 from 9:00 am to 5:00 p.m. Eastern Standard Time.

Sincerely,

Benjamin Schimelman
Associate General Counsel
UnitedHealthcare Privacy Office

[PLACEHOLDER FOR EXPERIAN LETTER]

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

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 P.O. Box 105788 Atlanta, GA 30348 Equifax Freeze Request Form *Mail the freeze request form to the address listed above.	Automated line: 1-800-349-9960 Customer Care: 1-888-298-0045	https://www.equifax.com/personal/credit-report-services/credit-freeze//
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

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.