

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



August 22, 2022

Dawna Kokosinski, Chief Market Analyst
Maryland Insurance Administration
200 St. Paul Place,
Baltimore, MD 21202

Submitted Via:
dawna.kokosinski@maryland.gov

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

Idtheft@oag.state.md.us

RE: Privacy Breach Notification
UHC File #: 489932

Dear Sir or Madam:

UnitedHealthcare (“UHC” or “We”) are writing to inform you of a recent incident that affected a Maryland resident.

On June 30, 2022, the UnitedHealthcare Privacy Office (“UHC”) learned of an issue with the secure messaging system in the myuhc.com member portal. A system error caused the secure messaging system in the member portal to populate a limited number of mailboxes with messages intended for another individual. On August 10, 2022, UHC learned that one (1) Maryland resident was impacted as a result of this issue.

The information potentially disclosed by this issue included a combination of the Indiana resident’s first and last name, telephone number and email address. This issue did not involve disclosure of the Indiana resident’s member ID number, date of birth, Social Security number, driver’s license number, sensitive medical diagnosis or any financial account information.

There is no evidence to suggest that any affected individuals’ information has been misused in any way. However, we were unable to verify the viewing or acquisition of the member’s information and could not confirm that any information that may have been viewed was destroyed and not retained.

Written notice will be provided to the impacted Maryland resident on or before August 26, 2022. The notification letter recommends steps the impacted individual 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. A copy of the notice letter

that that will be sent to the Maryland resident is enclosed. Additionally, UHC is notifying other regulatory agencies as required.

Protecting the personal information of individuals is very important to us. Immediately upon learning of the issue, the messages were removed from the system to prevent further risk of disclosure. The mailboxes affected by the issue were rebuilt and it was confirmed the issue is no longer occurring. Further, the system is being monitored with an alert in place to immediately flag the issue should it occur again.

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

Sincerely,

A handwritten signature in blue ink, appearing to read 'Josh Devine', with a long horizontal stroke extending to the right.

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, CT 06103

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



August xx, 2022

Name
Address
Address

Dear Name,

We are writing to let you know about a privacy issue involving some of your health information. The UnitedHealthcare (“UHC”) Privacy Office learned on June 30, 2022, of an issue with the secure messaging system on the myuhc.com member portal. On August 10, 2022, we confirmed that some of your health information may have been disclosed as a result of this issue. We believe this issue may have occurred between January 2, 2020, and July 1, 2022.

The information that may have been viewed included a selection of the following information: your first and last name; telephone number; email address; employer name or group number; claims information including provider or pharmacy information, dates of service, and claim number; prescription drug information; and medical services or diagnosis information. This incident did not involve disclosure of your address, date of birth, Social Security number, driver’s license number, sensitive medical information, or financial account information.

Upon discovery, we took prompt action to investigate the matter. It was determined that a system error caused the secure messaging system within the myuhc.com member portal to populate a limited number of mailboxes with messages intended for another individual. Immediately upon learning of the issue, the messages were removed from the system to prevent further disclosures. We rebuilt the impacted secure message mailboxes and confirmed the issue is no longer occurring. The system is being monitored with an alert in place to immediately flag the issue should it occur again.

While we have no evidence that another individual viewed or misused your information, we cannot confirm that another individual did not view your information. As a precaution to protect against misuse of your health information, we recommend you regularly monitor account statements and the explanation of benefits statements that you receive from us to check for any unfamiliar health care services. If you notice any suspicious activity, please contact the number on your member identification card. If you do not regularly receive explanation of benefits statements, you may request that we send you these statements following the provision of any health care services in your name or plan number by contacting the number on your member identification card.

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, particularly medical services or medical bills that you do not recognize. If you notice any suspicious activity, contact the credit reporting agencies using the contact information provided in the attached Reference Guide. We suggest that 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 your personal health 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. Should you have any questions, please feel free to contact me at 702-304-6941. Thank you in advance for your cooperation.

Sincerely,

Sandra Haase
Investigations Lead, Associate Director
UnitedHealthcare Privacy Office

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

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
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@dbri.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.

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 ("UHC")

Name of person filing this Notice: Joshua Devine Phone Number: 860-702-6805

Email Address: joshua_devine@uhc.com

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

Please see the attached letter for information regarding an issue involving the secure messaging system within
UnitedHealthcare's myuhc.com member portal. This issue impacted one (1) Maryland member.

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 Joshua Devine 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: _____

Print Name: Joshua Devine

Company: UnitedHealthcare

Title: Associate General Counsel

Date: August 22, 2022