UnitedHealthcare Privacy Office
7440 Woodland Drive
IN020-1000
Indianapolis, IN 46278

[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 September 4, 2019, we learned that Equian, LLC, a vendor of ours, was the target of a phishing attack. We believe the incident occurred on July 26, 2019.

The information that was involved may include your full name, Social Security number, date of birth, home address, Medicare ID number, diagnosis codes, procedure codes, lab results, claim information, telephone number, email address, religion, and gender.

We deeply regret this incident and any inconvenience or concern that it may cause. Upon discovery, we took prompt action to investigate the matter. Equian immediately reset the password for the impacted email account, provided companywide training regarding security practices and phishing awareness, and implemented multi-factor authentication for all email accounts.

While there is no evidence that your information was used, as a precaution and to protect against misuse of your health information, we recommend that you regularly monitor the explanation of benefits statements that you receive from us, your bank and credit card statements and tax returns to check for any unfamiliar activity. If you notice any health care services that you did not receive listed on an explanation of benefits statement, please call the number on the back of your ID 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 us at the number listed on the back of your ID card. If you notice any suspicious activity on either your bank or credit card statement, or tax returns, please immediately contact your financial institution and/or credit card company, or relevant institution**.**

Additionally, to help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorks^{SM}. This product provides you with superior identity detection and resolution of identity theft. 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.

Furthermore, Equian has established a dedicated toll-free hotline that you can call if you have any questions. Please call **(833) 704-9385** toll free Monday – Friday from 9:00am to 9:00pm ET and weekends from 11:00am to 8:00pm ET. The toll free number has been created specifically to answer your questions about the incident.

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 our vendors 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.

Sincerely,

Jackie Cutshall, CIPP/US, FLMI, FLHC
Privacy Manager – UnitedHealthcare

To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorks[SM]. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **December 31, 2019** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: **www.experianidworks.com/credit**
- Provide your **activation code**: **[code]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(833) 704-9385** by **December 31, 2019.** Be prepared to provide engagement number **DB14653** as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your 12-month Experian IdentityWorks Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE[TM]**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **(833) 704-9385.** If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions

for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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.