

UnitedHealthcare Notifies Individuals of Data Security Incident

Minneapolis, MN (Sept. 1, 2023) – UnitedHealthcare (“UHC”) is reporting a data security incident that involves the personal health information of certain [state] residents.

While the personal information accessed varied by individual, it may have included a combination of names, member ID number, plan type, and county and state of residency. This incident did not involve the disclosure of social security numbers, driver’s license numbers or any financial account information.

On December 29, 2022, UHC discovered an unauthorized third party was able to access a UHC broker portal limited to certain parts of our business. We notified law enforcement and worked with them to investigate the matter.

On February 3, 2023, UHC confirmed the unauthorized party accessed information from the portal while attempting to divert funds intended for agents and/or brokers. Through its investigation, UHC determined the unauthorized third party was able to access certain personal information between December 1, 2022, and January 25, 2023.

UHC is committed to protecting our members’ and brokers’ information and maintaining the integrity of our systems. UHC placed additional safeguards on the UHC broker portal to help minimize the risk of a similar incident occurring in the future.

Affected individuals are being notified. Any suspicious activity should immediately be reported to their health plan or other relevant institution. Additionally, a dedicated toll-free hotline has been established to help answer any questions and can be reached at 800-669-1812 Monday through Friday between 8am – 5pm CST.

Frequently Asked Questions

- What happened?

On December 29, 2022, UHC became aware of suspicious activity on our internal broker portal. We quickly took steps to stop that activity and began an investigation right away. We learned an unauthorized third-party was able to make fraudulent accounts on behalf of UHC brokers and access the UHC broker portal. We believe the main goal of this fraudulent activity was to steal money from UHC, but the unauthorized third-party may have obtained your information in the process.
- Was I impacted by this event?

Notices were mailed on September 1, 2023 to those individuals whose personal information may have been involved and for whom there was sufficient contact information. If you received a notification letter, then some of your personal information may have been impacted. If you have not received a letter, it is possible that the letter has not yet arrived. It is also possible that your personal information was not involved in this event.
- When did the event occur?

We believe your information may have been disclosed between December 1, 2022, and January 25, 2023.
- Why am I only now being contacted?

Cybersecurity investigations and data review take time due to the complicated nature of the event. It was important a thorough investigation into the incident took place to confirm what happened and identify those individuals who may have been impacted.

Additionally, UHC engaged law enforcement to assist in the investigation and they issued what is known as a “law enforcement delay.” This law enforcement delay was issued as public notification of the event would have compromised their ability to actively investigate the matter.
- What steps were taken when the event was discovered?

As soon as the event was discovered, an investigation was immediately launched. Law enforcement was contacted. The UHC broker portal security controls were reviewed and enhanced to prevent this issue from occurring again.
- What kind of information was exposed in this event?

Due to the nature of the incident, we are unable to confirm types of data that were exposed on an individual basis, however, the information involved may have included member first and last name, UHC member ID number, Exchange member ID, plan effective dates, plan type, contract/PBP numbers, county and state, plan affiliation, and if applicable, the reason a member’s plan terminated.

This incident **did not** involve disclosure of a driver’s license number, Social Security number, or any financial account information.

- Are credit monitoring services available?

With no financial account information exposed as a result of the incident, credit monitoring services are not being offered at this time. However, individuals have been provided with information to assist them should they identify any fraudulent activity on their accounts including information on receiving a free copy of their credit reports, placing a fraud alert on their credit file, or freezing their credit.
- What steps can I take to protect myself?

The Reference Guide enclosed with your letter contains additional information on general steps you can take to monitor and help safeguard your personal information. If you believe you are the victim of a crime, you can contact your local law enforcement authorities and file a police report. The Reference Guide is also included below.
- I received a letter in the mail. Is this fraudulent, a scam or a real incident?

Federal and state laws require notices of data breaches be sent to affected individuals. The letter received is intended to notify of a real event and provide you with information related to the event. Additionally, you are encouraged to carefully review the Reference Guide included in your notification letter for more information on general steps you can take to monitor and help safeguard your personal information.
- Who can I call if I have questions?

If you have any questions or concerns, please call us toll-free at 1-800-669-1812 from Monday through Friday between 8 a.m. – 5 p.m. CST.

Additional Resources/Reference Guide

Review Your Account Statements

Remain vigilant for incidents of potential fraud and identity theft. Carefully review account statements and credit reports to make sure that all your account activity is valid. Report any questionable charges promptly to the financial institution or company with which you maintain the account.

As a precaution to protect against misuse of your health information, we recommend that you remain vigilant and regularly monitor the explanation of benefits statements that you receive from your plan, and your bank and credit card statements, credit reports, 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 contact your plan. 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 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.

Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number, or request form.

Upon receiving your credit report, review them carefully. Look for any accounts you did not open. Look in the "inquires" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for inaccuracies in information (such as home address and Social Security number).

If you see anything that you do not understand, call the credit bureau at the telephone number of the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in your financial accounts, promptly notify the appropriate payment 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 FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

Federal Trade Commission
 Consumer Response Center
 600 Pennsylvania Avenue, NW
 Washington, DC 20580
 1-877-IDTHEFT (438-4338)
 1-866-653-4261 (TTY)
<https://consumer.ftc.gov/features/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 credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be a victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging your file with a fraud alert at all three bureaus.

Credit Agency	Mailing Address	Phone Number	Website
Equifax	P.O. Box 105069 Atlanta, GA 30348-5069	1-888-766-0008	www.equifax.com
Experian	P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

Place a Security Freeze on Your Credit File

You may wish to place a “security freeze” on your credit file, at no cost to you, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a credit

report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) phone number, current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

You can request a security freeze for free by contacting the credit bureaus at:

Credit Agency	Mailing Address*	Phone Number	Website
Equifax	P.O. Box 105788 Atlanta, GA 30348	1-800-349-9960	www.equifax.com
Experian	P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	1-800-916-8800	www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

Additional Attorney General Office Identity Theft Resources. You can obtain information from your state’s Attorney General’s Office about security breach response and steps 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, Office of Consumer Protection, 400 6th Street, NW, Washington DC 20001, 1-202-442-9828, <https://oag.dc.gov/consumer-protection/consumer-alert-identity-theft>.

For Iowa Residents. You may contact law enforcement or the Iowa Attorney General’s office to report suspected incidents of identity theft. The Iowa Attorney General’s Office can be reached at:

Iowa Attorney General’s Office

Director of Consumer Protection Division
1305 E. Walnut Street
Des Moines, IA 50319
Phone: 1-515-281-5926
Website: www.iowattorneygeneral.gov

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
Website: <https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>

For Residents of Massachusetts. You have the right to obtain a police report with respect to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For New Mexico Residents: New Mexico consumers have the right to obtain a security freeze or submit a declaration of removal.

You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

- (1) the unique personal identification number, password or similar device provided by the consumer reporting agency;
- (2) proper identification to verify your identity; and
- (3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

For New York Residents. You may also obtain information about security breach response and identity theft prevention and protection from the New York Attorney General's Office:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
Phone: 1-800-771-7755
Website: www.ag.ny.gov

For North Carolina Residents. You can obtain information about preventing and avoiding identity theft from 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: <https://ncdoj.gov/protecting-consumers/protecting-your-identity/>

For Oregon Residents. State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Department of Justice at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301
Phone: 1-877-877-9392
Website: www.doj.state.or.us

For Rhode Island Residents. You have a right to file or obtain a police report related to this incident. You may also obtain information about preventing and avoiding identity theft from 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

Website: <http://www.riag.ri.gov/ConsumerProtection/About.php#>