



September 21, 2022

Office of the Attorney General
Idtheft@oag.state.md.us

RE: Humana #502712

NOTICE OF CYBERSECURITY INCIDENT

Dear Attorney General,

Humana has a contract with Choice Health to sell Medicare products on our behalf. On May 14, 2022, Choice Health learned that an unauthorized person was offering to make data available that was allegedly taken from a Choice Health database.

What Happened?

On May 18, 2022, Choice Health determined that, due to a technical security configuration issue caused by a third-party service provider, a single Choice Health database was accessible through the Internet. Based on their investigation, an unauthorized individual accessed this database and obtained certain database files on or about May 7, 2022. At the time, Choice Health believed the affected data was comprised solely of lead generation and marketing information that belonged exclusively to Choice Health and not to any of their carrier partners.

Consistent with their findings, on June 8, 2022, Choice Health sent notification letters to 3 Maryland state residents/impacted Humana members. Attached you will find a copy of the letter that includes an application for two years of free credit monitoring and identity theft protection. In accordance with Maryland and/or federal law, we have also notified the consumer reporting agencies and any other required agency.

On July 26, 2022, Choice Health determined that the data included carrier partners information, including Humana. On August 5, 2022, Choice Health notified Humana that Humana member data was impacted by this incident. Choice Health provided the impacted individual data list to Humana on August 29, 2022.

What Information Was Involved?

The files obtained by the unauthorized individual contained the following types of personal information, first and last name, Social Security number, Medicare beneficiary identification number, date of birth, address and contact information, and health insurance information.

What We Are Doing.

Upon learning of the incident, Choice Health worked with their third-party service provider to reconfigure the security settings on the database. The database is no longer accessible through the Internet. Choice Health has also taken steps to enhance their data security measures to prevent the occurrence of a similar event in the future, including requiring multi-factor authentication for all access to database files.

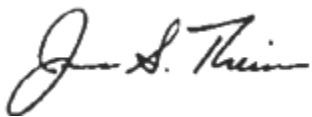
What Individuals Can Do.

Choice Health encouraged individuals to remain vigilant against incidents of identity theft and fraud by reviewing account statements and monitoring free credit reports for suspicious activity and to detect errors. An Identity Theft Guide was included with the mailing. It provided additional details on how to take steps to protect information, should an individual feel it is necessary to do so.

Humana will promptly report to your office and appropriate law enforcement officials any information that is shared with us that indicates this information has been inappropriately used.

Please do not hesitate to contact me if you have any additional questions regarding this situation.

Sincerely,



James S. Theiss
Associate VP, Privacy & Ethics
Humana Inc.
502-580-4322
jtheiss@humana.com

Attachments



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

June 8, 2022

H9725-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



RE: Notice of Data Breach. Please read this entire letter.

Dear Sample A. Sample:

At Choice Health, we are committed to protecting the confidentiality and security of your personal information. We are sending you this letter to let you know that Choice Health recently experienced a security incident that may have resulted in unauthorized access to your personal information. *At this time, we are not aware of any misuse of your personal information.*

What Happened? On May 14, 2022, Choice Health learned an unauthorized person was offering to make available data allegedly taken from Choice Health. We promptly began an investigation into the incident. On May 18, 2022, we determined that, due to a technical security configuration issue caused by a third-party service provider, a single Choice Health database was accessible through the Internet. Based on our investigation, an unauthorized individual accessed the database from the Internet and obtained certain database files on or about May 7, 2022. We are notifying you of this incident, because your personal information was in the database.

What Information Was Involved? The files obtained by the unauthorized individual contained the following types of personal information, some of which may have been included about you: first and last name, Social Security number; Medicare beneficiary identification number; date of birth; address and contact information; and health insurance information.

What We Are Doing? Upon learning of the incident, we promptly worked with our third-party service provider to reconfigure the security settings on the database, and we confirmed that the database is no longer accessible through the Internet. We have also taken steps to enhance our data security measures to prevent the occurrence of a similar event in the future, including requiring multi-factor authentication for all access to database files.

Although we have no reason to believe that your information has been misused because of this incident, we would like to offer you a complimentary 24-month membership of Experian IdentityWorksSM. 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** August 31st, 2022 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 888-829-6549 by August 31st, 2022. Be prepared to provide engagement number B054235 as proof of eligibility for the Identity Restoration services by Experian.

0000001



H9725-L01

Please review the sheet enclosed with this letter for information about activating Experian's IdentityWorks services.

What You Can Do. In addition to enrolling in Experian's IdentityWorks services, you should consider taking the following steps to protect yourself:

- Read account statements from your health care providers, explanations of benefits (EOBs) from your health plan and other documents related to medical services to make sure they do not include services you did not receive.
- Be attentive to documents related to medical services that you usually receive and that suddenly do not arrive, as you usually receive them.
- All mail related to medical or financial information should be destroyed and preferably shredded before you throw it away.
- Be careful when offering personal information over the phone, mail or internet, and unless you are sure of the person with whom you are dealing, offer as little information as possible.
- Review the "General Information About Identity Theft Protection" materials that are included with this letter. You should always remain vigilant for threats of fraud and identity theft by regularly reviewing your account statements and credit reports.

For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call 888-829-6549 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number B054235.

Sincerely,

C. Pappas

Colleen Pappas, Vice President
Choice Health

ADDITIONAL DETAILS REGARDING YOUR TWENTY-FOUR (24) MONTHS 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 specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$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 as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. 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 from the date of the incident (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 Identity Restoration is available to you for twenty-four (24) months 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.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary twenty-four (24) months membership.

* 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.



GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

You should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Credit Reports. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. **You may contact the nationwide credit reporting agencies at:**

Equifax

P.O. Box 105788
Atlanta, GA 30348
www.equifax.com
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
www.experian.com
(888) 397-3742

TransUnion

P.O. Box 2000
Chester, PA 19016
www.transunion.com
(800) 680-7289

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Place a Security Freeze on your Credit Report. You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed at above. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line or a written request. 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) 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. You can place a freeze and lift a security freeze on your credit report free of charge.

You may contact the Federal Trade Commission (FTC) and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the FTC and/or your state's attorney general office about for information on how to prevent or avoid identity theft. You can contact the FTC at: **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20508, www.ftc.gov, 1-877-IDTHEFT (438-4338).

For District of Columbia Residents: District of Columbia Office of the Attorney General, 400 6th St. NW, Washington, DC 20001, <https://oag.dc.gov>, (202) 727-3400

For Iowa Residents: State law advises you to report any suspected identity theft to law enforcement or to the Iowa Attorney General, Consumer Protection Division, 1305 E. Walnut St., Des Moines, IA 50319, 1-888-777-4590

For Maryland Residents: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023

For Massachusetts Residents: You have the right to obtain a police report if you are the victim of identity theft.

For New Mexico Residents: You have certain rights pursuant to the federal Fair Credit Reporting Act (FCRA). For more information about the FCRA, please visit www.ftc.gov

For North Carolina Residents: North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com, 1-877-566-7226