Mutual of Omaha

Omaha Health Insurance Company
A Mutual of Omaha Company

3300 Mutual of Omaha Plaza
Omaha, NE 68175

August 2, 2023

CONFIDENTIAL – INTENDED FOR ADDRESSEE ONLY

Via Email
Maryland Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Re: Notification of Data Security Incident

Dear Maryland Office of the Attorney General:

We are writing to inform you of an incident that involved the disclosure of personal information as required under Md. Code Com. Law §14-3501-3508. The details of the incident are described below.

Facts of the data security incident:
Omaha Health insurance Company ("OHIC") was notified on June 22, 2023, that one of its vendors discovered a security incident that potentially involved OHIC member information. The vendor was notified of a zero-day vulnerability on its MoveIT file transfer software by the MoveIT company on June 2, 2023. The vendor immediately initiated an investigation of the vulnerability on June 2, 2023. The vendor did not confirm until June 22, 2023, that multiple downloads had been made by an unknown, unauthorized party between May 30, 2023, and June 2, 2023. OHIC was notified on June 29, 2023, that the security incident involved OHIC member personal information. OHIC was provided a detailed list of compromised member information by the vendor on July 13, 2023.

Mitigation and preventative measures by vendor:
Upon discovery of the security incident, the following measures were taken:

- All recommended ports were blocked, and patches were applied for the MOVEit transfer server.
- Firewall rules were configured to deny HTTP and HTTPS traffic to the MOVEit Transfer server.
- The vendor promptly engaged a third-party forensic firm to complete a full forensic investigation for the MOVEit transfer server. This investigation identified no lateral movement or no signs of additional impact.
- Web shells and all other artifacts discovered during forensic analysis were removed.
- All MOVEit passwords and active sessions were reset multiple times.
- The vendor rebuilt the server that hosted MOVEit Transfer on July 6, 2023.
- There has been no evidence of unauthorized downloads or access to the MOVEit transfer server since June 2.

Steps OHIC has taken:
Upon receiving the results of the third-party forensic review, OHIC immediately analyzed the vendor report and determined that a breach under Maryland law occurred. OHIC has no evidence that any individual was adversely impacted or that the potentially impacted information has been misused. OHIC is working closely with the vendor to ensure systems are updated to block these activities and prevent disclosures of this nature from occurring in the future.

Information Involved and Number of Individuals. Based on information provided to OHIC by our vendor, the incident involved the personal information for 115 Maryland residents. The downloaded data will differ depending on the individual but may include personal information such as name, mailing address, email address, phone number, [date of birth], [Social Security Number], [medical claims information], [banking information], [billing information], and/or [medical treatment information].

OHIC will provide notification of this incident to potentially impacted individuals. The notification letter will be sent on August 3, 2023 via USPS First Class Mail, and offers complimentary identity protection services and provides information to the individuals on steps that can be taken to protect their personal information. A sample notification letter is enclosed.

We sincerely regret any inconvenience or concern caused by this incident. The privacy and security of our customers' information is of critical importance to us. If you have further questions or need additional information about this incident, you may contact us at 1-844-213-3454.

Sincerely,

Polly Faltin
Manager Privacy

Enc: Sample Notification Letter

802 N. Carancahua St. Suite 800
Corpus Christi, TX 78401

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:

https://response.idx.us/notice-info

Date,

«Individuals_First_Name» «Individuals_Last_Name»
«Individuals_Street_Address»
«Individuals_City», «Individuals_State» «Individuals_Zip_Code»

Re: **NOTICE OF DATA BREACH - PLEASE READ CAREFULLY**

Dear «Individuals_First_Name» «Individuals_Last_Name»:

Your HealthPlan/Pharmacy Benefits Manager, Omaha Health insurance Company ("OHIC"), is providing this letter to you with specific details about a recent unauthorized release of your personal information, including protected health information (PHI), related to your Medicare Part D Prescription Drug Plan with OHIC and issued under the name of Mutual of Omaha Rx℠ (PDP)*. This letter is required by privacy provisions under applicable laws.

What occurred:
On June 22, 2023, OHIC was notified that one of its vendors discovered a security incident on June 21, 2023. The vendor immediately initiated an investigation that confirmed that multiple downloads had been made by an unauthorized party between May 30, 2023 and June 2, 2023.

What Data was involved:
Based on information provided to OHIC by our vendor, we have determined that the downloaded data may include your name and one or more of the following pieces of information: mailing address, email address, phone number, [date of birth], [Social Security Number], [medical claims information], [banking information], [billing information], and/or [medical treatment information].

Steps we have taken:
OHIC is working closely with the vendor to ensure systems are updated to block these activities and prevent disclosures of this nature from occurring in the future. OHIC sincerely regrets any inconvenience or concern cause by this incident and is committed to maintaining the privacy and security of your information. **We are taking this incident very seriously** and our vendor has notified law enforcement to mitigate this situation as best as possible.

Although we have no indication that your personal information has or will be misused as a result of this incident, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling (888) 727-2311, going to https://response.idx.us/notice-info, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is 3 months from the date of this letter.

Steps you can take:
We recommend you monitor your accounts and watch for any suspicious activity. If you suspect or discover that your information has been used inappropriately, please notify your local law enforcement or consumer protection agency.

Again, we regret that this incident occurred as OHIC takes the confidentiality of its members' data very seriously. If you have any questions or learn of additional information you may visit our website at https://response.idx.us/notice-info or call (888) 727-2311, We have also prepared a list of frequently asked questions which you may find helpful, and which can be accessed online at https://response.idx.us/notice-info.

Sincerely,

Nichole Hageman
Compliance Officer

*Mutual of OmahaRx is a prescription drug plan with a Medicare contract. Enrollment in Mutual of OmahaRx depends on contract renewal.

ADDITIONAL INFORMATION

You should always remain vigilant, including by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions.

In addition, you may contact the Federal Trade Commission (FTC) or law enforcement, including your Attorney General, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's website, at www.consumer.gov/idtheft, or call the FTC, at (877) IDTHEFT (438-4338) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

For resident of Maryland: Consumer may obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oga.state.md.us.

You may also periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under the federal Fair Credit Reporting Act (FCRA), you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies regardless of whether you've experienced an identity theft incident or not. You may obtain your annual free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(888) 909-8872

P.O. Box 740241	P.O. Box 9701	Fraud Victim Assistance Division
Atlanta, GA 30374-0241	Allen, TX 75013	P.O. Box 2000
Equifax.com/personal/	Experian.com/help	Chester, PA 19022
credit-report-services		TransUnion.com/credit-help

In addition, you may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. In addition, you can contact the nationwide credit reporting agencies at the following numbers to place a security freeze to restrict access to your credit report:

(1) Equifax – (800) 685-1111
(2) Experian – (888) 397-3742
(3) TransUnion – (888) 909-8872

You will need to supply your name, address, date of birth, Social Security number and other personal information to each credit reporting agency. After receiving your request, each credit reporting agency will send you a confirmation letter containing a unique PIN or password that you will need in order to lift or remove the freeze. You should keep the PIN or password in a safe place.