

October XX, 2024

Omni Family Health
4900 California Ave #400-B
Bakersfield, CA 93309

[Patient/Former Patient Full Name]
[Address Line 1 & 2]
[City, State, Zip Code]

RE: Notice of Data Breach

Dear [Patient/Former Patient's Full Name]:

Omni Family Health ("Omni") is writing to inform you of a recent security incident involving your personal information. Omni may maintain your information if you are a current or former patient of Omni, or if you were referred to Omni for healthcare services.

While we are unaware of any reports of fraud or identity theft as a result of this incident, we are sending this notice to potentially affected individuals. We encourage you to read this letter carefully as it contains information regarding the incident and steps you can take to safeguard your personal information.

Please be assured, all health centers remain open during normal business hours and our providers and staff continue to operate safely and securely.

What Happened?

On August 7, 2024, we became aware of claims that information was taken from our systems and posted on the dark web. The dark web is a hidden part of the internet that is not accessible through regular search engines like Google. Upon learning of these claims, we immediately initiated an investigation and engaged outside cybersecurity specialists to assist with our efforts. We also notified federal law enforcement.

Through the investigation, Omni determined the data posted on the dark web appeared to be related to Omni's patients and employees. Consequently, we are notifying individuals whose information could be included in the posted data.

What Information Was Involved?

The information impacted for each individual varies. If you are a current or former patient of Omni, or were referred to Omni for medical care, the following types of information related to you were potentially involved in this incident: name, address, Social Security number, date of birth, health insurance plan information, and medical information.

What We Are Doing.

The confidentiality, privacy, and security of information maintained by Omni remains our top priority. Upon becoming aware of the claims of information on the dark web, we moved quickly and diligently to investigate the claims, ensure the security of our systems, and identify whose information may be included in the dark web posting.

We strongly encourage you to review the steps outlined in this letter to protect your information and sign up for the services being offered. Cybersecurity is an ongoing concern for everyone, as companies worldwide face cybersecurity threats. Individuals can better protect themselves by following the steps below.

For a small population of individuals, it is possible you are receiving this letter out of an abundance of caution and your data was not involved. This precautionary measure was taken to ensure that anyone who could have been affected by the incident received notice. Regardless, we still strongly encourage you to review the steps outlined in this letter to protect your information and sign up for the services being offered.

What You Can Do.

Although Omni is not aware of any claims that individuals have been victims of fraud as a result of this incident, we are encouraging individuals to take steps to protect their personal information and are also offering individuals access to 12 months of complimentary credit monitoring and identity protection services through Experian. Additional information pertaining to these services and enrollment instructions are provided below.

1. Register for Identity Protection Services. [Insert Vendor Specific Enrollment Instructions].

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for [##] months.

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 [##] 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 [##]-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** [Enrollment End Date] (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [Enrollment URL]
- Provide your **activation code**: [Activation Code]

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 1-877-288-8057 by [Enrollment End Date]. Be prepared to provide engagement number [B#####] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [##]-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, Equifax and Transunion files 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.
2. Review Your Accounts for Suspicious Activity. We encourage you to remain vigilant by regularly reviewing your accounts and monitoring credit reports for suspicious activity.
 3. Order a Credit Report. If you are a U.S. resident, you are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. 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. Contact information for the nationwide credit reporting agencies is provided in the next section.
 4. Contact the Federal Trade Commission, Law Enforcement and Credit Bureaus. You may contact the Federal Trade Commission (“FTC”), your state’s Attorney General’s office, or law enforcement, 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 websites at www.identitytheft.gov and; call the FTC at (877) IDTHEFT (438-4338); or write to: FTC Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may contact the nationwide credit reporting agencies at:

- a) **Equifax:** (800) 525-6285; P.O. Box 740241, Atlanta, Georgia, 30374; or www.equifax.com.
 - b) **Experian:** (888) 397-3742; P.O. Box 9701, Allen, TX 75013; or www.experian.com.
 - c) **TransUnion:** (800) 916-8800; Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19022; or www.transunion.com.
5. Additional Rights Under the FCRA. You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here.

Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by: (i) visiting https://files.consumerfinance.gov/f/documents/bcbp_consumer-rights-summary_2018-09.pdf ; or (ii) by writing to Consumer Financial Protection Bureau, 1700 G Street, N.W., Washington, DC 20552.

6. Request Fraud Alerts and Security Freezes. 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 at no cost to you:

- a) Equifax: (800) 349-9960
- b) Experian: (888) 397-3742
- c) TransUnion: (888) 909-8872

Placing a security freeze prohibits the agency from releasing any information about your credit report without your written authorization. Security freezes must be placed separately at each of the three nationwide credit reporting agencies. When requesting a security freeze, you may need to provide the following information:

- Your full name, with middle initial as well as Jr., Sr., II, etc.
- Social Security number
- Date of birth
- Current address and all addresses for the past two years
- Proof of current address, such as a current utility bill or telephone bill
- Legible copy of a government-issued identification card, such as a state driver's license, state identification card, or military identification.

After receiving your request, each agency will send you a confirmation letter containing a unique PIN or password that you will need to lift or remove the freeze. You should keep the PIN or password in a safe place.

For More Information.

We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call the dedicated, toll-free call center number at 855-507-8493, Monday through Friday from 6:00 a.m. to 6:00 p.m. Pacific Time, excluding major U.S. holidays, to enroll in credit monitoring services.

Safeguarding the information maintained by Omni Family Health remains our top priority. We value our patients and sincerely regret any inconvenience or concern this event may cause you.

Sincerely,

Omni Family Health