



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Elizabeth Dill
Office: (267) 930-5327
Fax: (267) 930-4771
Email: edill@mullen.law

4870 Sadler Road, Suite 300
Glen Allen, VA 23060

August 12, 2022

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent United Health Centers of the San Joaquin Valley (“UHC”) located at 3875 West Beechwood Avenue, Fresno, California 93722, and are writing to notify your office of an incident that may affect the security of certain personal information relating to seven (7) Maryland residents. By providing this notice, UHC does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On August 28, 2021, UHC experienced technical difficulties resulting in a disruption to certain computer systems. UHC promptly took steps to secure its systems and commenced an investigation into the nature and scope of the incident. UHC’s investigation determined that the disruption was caused by an encryption event. UHC worked expeditiously to restore its systems to avoid an interruption to patient care.

On September 22, 2021, UHC discovered that certain UHC-related data may have been compromised. UHC immediately undertook a further investigation, with the assistance of third-party specialists, to confirm the scope of the incident. The investigation determined that certain UHC-related data was compromised between August 24, 2021 and August 28, 2021. With the assistance of third-party subject matter specialists, UHC then undertook a diligent and thorough review of the impacted documents to determine what information these documents contained and to whom that information related. UHC completed this review on April 11, 2022 and then worked expeditiously to locate address information and provide written notice to those individuals whose information was found within the documents.

The information that could have been subject to unauthorized access includes name, Social Security number, medical record number, health information, and health insurance information.

Notice to Maryland Residents

On August 2, 2022, UHC determined that the incident involved the information of seven (7) Maryland residents. On or about August 12, 2022, UHC provided written notice of this incident to those residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, UHC moved quickly to investigate and respond to the incident, assess the security of UHC systems, and identify potentially affected individuals. Further, UHC notified federal law enforcement regarding the event UHC is also working to implement, and has already implemented, additional safeguards and training to its employees.

Additionally, UHC is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. UHC is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

UHC is providing written notice of this incident to relevant state regulatory authorities, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. UHC has also notified the U.S. Department of Health and Human Services and prominent media pursuant to the Health Insurance Portability and Accountability Act (HIPAA), on November 19, 2021. On October 14, 2021, UHC also published notice of the incident on its website.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-5327.

Very truly yours,

Elizabeth Dill of
MULLEN COUGHLIN LLC

ERD/ams
Enclosure

EXHIBIT A

United Health Centers of the
San Joaquin Valley
c/o A.B. Data, Ltd.
P.O. Box 173005
Milwaukee, WI 53217

FIRST CLASS
PRESORT
US POSTAGE
PAID
PERMIT NO. 3780
MILWAUKEE WI

A

August 12, 2022

NOTICE OF DATA INCIDENT

United Health Centers of the San Joaquin Valley (“UHC”) is writing to notify you of an event that may affect your information. This letter provides information about the event, our response, and the resources we are making available to you to help protect your information, should you feel it appropriate to do so.

What Happened? On August 28, 2021, UHC experienced technical difficulties resulting in a disruption to certain computer systems. UHC promptly took steps to secure our systems and commenced an investigation into the nature and scope of the incident. UHC’s investigation determined that the disruption was caused by an encryption event. UHC worked expeditiously to restore our systems to avoid an interruption to patient care.

On September 22, 2021, UHC discovered that certain UHC-related data had been compromised. UHC immediately undertook a further investigation, with the assistance of third-party specialists, to confirm the scope of the incident. The investigation determined that certain UHC-related data was compromised between August 24, 2021 and August 28, 2021. With the assistance of third-party subject matter specialists, we then undertook a diligent and thorough review of the impacted documents to determine what information these documents contained and to whom that information related. We completed this review on April 11, 2022, and then worked expeditiously to provide notice to those patients whose information was found within the documents.

What Information Was Involved? Our investigation determined that your name and date of birth, medical record number and medical treatment/diagnosis information were present within the impacted documents.

What We Are Doing. The confidentiality, privacy and security of information within our care are among UHC’s highest priorities. We moved quickly to investigate and identify any impacted information. We have notified federal law enforcement, as well as appropriate regulatory authorities, and are notifying affected individuals, including you, to provide information on steps you can take to protect your information.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity and to detect errors. We also recommend you review the *Steps You Can Take to Protect Your Personal Information* section of this letter.

For More Information. We understand that you may have questions about this incident that are not addressed in this notice. If you have additional questions or concerns, please call our toll-free dedicated assistance line at 1-877-354-3821. This toll free line is available Monday - Friday 8:00 AM to 5:00 PM CST. You may also write to UHC at 3875 West Beechwood Avenue, Fresno, California 93722.

We sincerely regret any inconvenience this event may cause you. We appreciate your trust in us and remain committed to safeguarding the information in our care.

Sincerely,

United Health Centers of the San Joaquin Valley

DEV

STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	Transunion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances

of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. UHC is located at 3875 West Beechwood Avenue, Fresno, California 93722.

For New Mexico residents, 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 bureaus 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 violator. 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 visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 2 Rhode Island residents impacted by this incident.

DEV