

NOTICE OF DATA BREACH

AltaMed Health Services Corporation (“AltaMed”) is providing notice of an incident that may affect the privacy of personal information. This notice provides details of the incident, our response, and steps individuals may take to better protect against possible misuse of their personal information, should they feel it appropriate to do so.

On August 9, 2024, AltaMed became aware of suspicious activity on its computer systems. AltaMed quickly took steps to stop the activity, disconnect the systems to prevent further impact, and investigate the matter. Further, AltaMed launched a detailed investigation to determine the nature and scope of certain suspicious email related activity. The investigation determined that an unauthorized individual gained access to a certain email account between August 5 and August 9, 2024. AltaMed then undertook a comprehensive and time-intensive review of the potentially impacted data with the assistance of additional data security specialists to identify the information contained within, identify the individuals whose information may have been impacted, and identify accurate address information for potentially impacted individuals. On April 16, 2025, AltaMed finalized this review. To date, we have seen no evidence of any fraudulent use of data as a result of this event.

AltaMed takes the confidentiality, privacy, and security of information in its care very seriously. Upon learning of the event, we immediately commenced an investigation and took steps to implement additional safeguards and review our policies and procedures relating to data privacy and security.

The investigation determined the types of information potentially impacted for certain individuals includes name and one or more of the following: **Social Security number, date of birth, driver's license number, Passport number, foreign national ID number, personal email, personal telephone, medical record number, Medicare or Medicaid ID, medical billing information, doctor or provider name, date of service, payment for health services, medical history, medical treatment information, mental or physical condition or diagnosis, procedure information, COVID test result or vaccination status, prescription information, incidental health reference, health insurance policy number, other health insurance information, handwritten or signature, genetic data, mother's maiden name, and username and password.**

AltaMed is mailing letters to potentially affected individuals for whom it has an address.

If you have questions, please call 1-800-939-4170 Monday through Friday from 6:00 AM – 6:00 PM Pacific, excluding holidays. You may also write to AltaMed Health Services Corporation Attn: Legal Department, at 2040 Camfield Ave., Los Angeles, CA 90040.

STEPS YOU CAN TAKE TO PROTECT 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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which

is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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 they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, 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/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, 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, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.