

AltaMed

P.O. Box 989728

West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip>>

<<Country>>

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

June 13, 2025

NOTICE OF <<Variable Text 1: SECURITY INCIDENT / DATA BREACH>>

Dear <<First Name>> <<Last Name>>:

AltaMed Health Services Corporation (“AltaMed”) is writing to notify you of an incident that may have impacted your personal information. This letter provides details of the incident, our response, and steps you may take to help protect against the possible misuse of your information should you feel it is appropriate to do so.

What Happened?

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.

What Information Was Involved?

The information potentially impacted by this incident includes your name and <<Variable Text 3: Data Elements English>>.

What We Are Doing.

AltaMed takes the confidentiality, privacy, and security of information in its care very seriously. Upon learning of the event, AltaMed conducted a diligent investigation to confirm the full nature and scope, took prompt steps to ensure security of its email environment, and conducted a comprehensive review of the information potentially affected. AltaMed also enhanced its existing security protocols. AltaMed continues to evaluate its policies and procedures related to data privacy and security.

As an added precaution, AltaMed is providing you with access to credit monitoring services for twenty-four (24) months at no cost to you. Information on these services and instructions on how to activate them may be found in the enclosed *Steps You Can Take to Help Protect Your Personal Information*. Please note that you must complete the enrollment process as we are not permitted to enroll you in these services.

What You Can Do.

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits and monitoring your free credit reports for suspicious activity and to detect errors over the next twenty-four (24) months.

For More Information.

We understand you may have questions about the incident that are not addressed in this letter. 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.

Sincerely,

AltaMed Health Services Corporation

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

- 1. Website and Enrollment.** Scan the QR image or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
- 2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
- 3. Telephone.** Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

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

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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, individuals have the right to obtain any police report filed in regard to this event. There are approximately 0 Rhode Island residents that may be impacted by this event.



P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Código de inscripción: <<ENROLLMENT>>

Para inscribirse, escanee el código QR a continuación:



o visite:

<https://app.idx.us/account-creation/protect>

June 13, 2025

AVISO DE <<Variable Text 1: SECURITY INCIDENT / DATA BREACH>>

Estimado <<First Name>> <<Last Name>>:

AltaMed Health Services Corporation (“AltaMed”) se comunica para notificarle de un incidente que podría haber afectado a su información personal. Esta carta proporciona detalles sobre el incidente, nuestra respuesta y las medidas que puede tomar para ayudar a proteger su información contra un posible uso indebido, si lo considera oportuno.

¿Qué sucedió?

El 9 de agosto de 2024, AltaMed detectó una actividad sospechosa en sus sistemas informáticos. AltaMed tomó rápidamente medidas para detener la actividad, desconectar los sistemas para evitar más repercusiones e investigar el asunto. Además, AltaMed puso en marcha una investigación detallada para determinar la naturaleza y el alcance de cierta actividad sospechosa relacionada con el correo electrónico. La investigación determinó que una persona no autorizada accedió a una determinada cuenta de correo electrónico entre el 5 y el 9 de agosto de 2024. A continuación, AltaMed llevó a cabo una revisión exhaustiva y minuciosa de los datos que podrían haberse visto afectados, con la ayuda de especialistas adicionales en seguridad de datos, con el fin de identificar la información contenida en ellos, identificar a las personas cuya información podría haberse visto afectada e identificar la información de dirección precisa de las personas que podrían haberse visto afectadas. El 16 de abril de 2025, AltaMed finalizó esta revisión. Hasta la fecha, no hemos encontrado pruebas de ningún uso fraudulento de los datos como resultado de este incidente.

¿De qué información se trató?

La información que podría verse afectada por este incidente incluye su nombre y los <<Variable Text 4: Data Elements Spanish>>.

¿Qué estamos haciendo?

AltaMed se toma muy en serio la confidencialidad, la privacidad y la seguridad de la información que tiene a su cargo. Al tener conocimiento del incidente, AltaMed llevó a cabo una investigación diligente para confirmar su naturaleza y alcance, tomó medidas inmediatas para garantizar la seguridad de su entorno de correo electrónico y realizó una revisión exhaustiva de la información que pudiera verse afectada. AltaMed también mejoró sus protocolos de seguridad existentes. AltaMed sigue evaluando sus políticas y procedimientos relacionados con la privacidad y la seguridad de los datos.

Como precaución adicional, AltaMed le proporciona acceso a servicios de monitoreo de crédito durante veinticuatro (24) meses sin costo alguno para usted. La información sobre estos servicios y las instrucciones para activarlos se

pueden encontrar en el documento adjunto *Pasos que puede tomar para ayudar a proteger su información personal*. Tenga en cuenta que debe completar el proceso de inscripción, ya que no se nos permite inscribirlo en estos servicios.

¿Qué puede hacer usted?

Le recomendamos que permanezca alerta ante incidentes de robo de identidad y fraude revisando sus estados de cuenta y la explicación de los beneficios, y monitoreando sus informes de crédito gratuitos para detectar actividades sospechosas y errores durante los próximos veinticuatro (24) meses.

¿Cómo obtener más información?

Entendemos que usted puede tener preguntas sobre el incidente que no se tratan en esta carta. Si tiene preguntas, llame al 1-800-939-4170 de lunes a viernes de 6:00 AM – 6:00 PM Pacífico, excepto los días feriados. También puede escribir a AltaMed Health Services Corporation, a la atención de: Legal Department, at 2040 Camfield Ave., Los Angeles, CA 90040.

Cordialmente,

AltaMed Health Services Corporation

Inscribirse en el servicio de monitoreo

1. Sitio web e inscripción: Escanee la imagen QR o vaya a <https://app.idx.us/account-creation/protect> y siga las instrucciones para inscribirse utilizando su Código de Inscripción proporcionado en la parte superior de la carta.

2. Active el monitoreo de crédito provisto como parte de su membresía de protección de identidad de IDX. Para que entrase en vigencia, el monitoreo incluido en la membresía se debe activar. Nota: Debe contar con crédito establecido y acceso a una computadora e Internet para utilizar este servicio. Si necesitara ayuda, IDX podrá ayudarlo.

3. Teléfono: comuníquese con IDX al 1-800-939-4170 para obtener información adicional sobre este incidente y hablar con representantes con conocimientos del tema sobre las medidas que debe adoptar para proteger su identidad crediticia.

Monitoree sus cuentas

Según las leyes de los Estados Unidos de Norteamérica, el consumidor tiene derecho a un informe crediticio gratuito anual de cada una de las tres principales agencias de informes crediticios, Equifax, Experian y TransUnion. Para solicitar un informe de crédito gratuito, visite www.annualcreditreport.com o llame al número gratuito 1-877-322-8228. Los consumidores pueden comunicarse directamente con las tres principales agencias de informes crediticios indicadas a continuación para solicitar una copia gratuita de su informe de crédito.

Los consumidores tienen derecho a colocar una “alerta de fraude” inicial o prolongada en un expediente crediticio de manera gratuita. Una alerta de fraude inicial es una alerta de un año que se coloca en el expediente crediticio de un consumidor. Al ver una alerta de fraude en el expediente crediticio de un consumidor, una compañía debe tomar medidas para verificar la identidad del consumidor antes de otorgarle un crédito nuevo. Si los consumidores resultan víctimas de un robo de identidad, tienen derecho a una alerta de fraude prolongada, que es una alerta de fraude de una duración de siete años. Si los consumidores desearan colocar una alerta de fraude, deben comunicarse con cualquiera de las tres agencias principales de informes de crédito que se indican a continuación.

Como alternativa a una alerta de fraude, los consumidores tienen derecho a realizar un “congelamiento de crédito” sobre un informe de crédito, lo cual impedirá que una agencia de crédito divulgue información del informe crediticio sin la autorización expresa del consumidor. El congelamiento de crédito está diseñado para evitar que se aprobasen créditos, préstamos y servicios en nombre del consumidor sin su consentimiento. Sin embargo, los consumidores deben tener en cuenta que el uso de un congelamiento de crédito para tener control de quién tiene acceso a la información personal y financiera de su informe de crédito puede retrasar, impedir o interferir en la aprobación oportuna de alguna solicitud o aplicación posterior que hicieran en relación con un nuevo préstamo, crédito, hipoteca o cualquier otra cuenta que implicase la ampliación del crédito. De conformidad con las leyes federales, a los consumidores no se les puede cobrar por colocar o levantar un congelamiento de crédito sobre su informe de crédito. Para solicitar un congelamiento del crédito, es posible que las personas deban proporcionar toda o parte de la siguiente información:

1. nombre completo (incluida la inicial del segundo nombre, así como Jr., Sr., II, III, etc.);
2. número de Seguro Social;
3. fecha de nacimiento;
4. direcciones de los últimos dos a cinco años;
5. prueba del domicilio actual, como una factura de servicios públicos o de teléfono;
6. una fotocopia legible de una tarjeta de identificación emitida por el gobierno (licencia de conducir o tarjeta de identificación del estado, etc.) y
7. una copia de la denuncia policial, del informe de la investigación o de la denuncia a una agencia del orden público sobre el robo de identidad, en caso de ser víctima de este delito.

Si los consumidores desearan realizar un congelamiento de crédito o colocar una alerta de fraude, deben comunicarse con las tres principales agencias de informes crediticios que se indican a continuación:

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

Información adicional

Los consumidores pueden informarse mejor sobre el robo de identidad, las alertas de fraude, los congelamientos de crédito y las medidas que pueden tomar para proteger su información personal al comunicarse con las agencias de informes del consumidor, la Comisión Federal de Comercio (Federal Trade Commission) o el Fiscal general de su estado. La información de contacto de la Comisión Federal de Comercio es la siguiente: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338) y teléfono de texto (text telephone, TTY): 1-866-653-4261. La Comisión Federal de Comercio también recomienda a quienes descubriesen que su información se ha utilizado de manera indebida que presenten una queja a su oficina. Los consumidores pueden obtener más información sobre cómo presentar dicha queja por medio de la información de contacto mencionada con anterioridad. Si alguna vez los consumidores sufriesen un robo de identidad o un fraude, tienen derecho a presentar una denuncia policial. Tenga en cuenta que, para presentar una denuncia a las autoridades policiales por robo de identidad, los consumidores probablemente tendrán que proporcionar alguna prueba de que han sido víctimas de dicho delito. Los casos de robo de identidad conocidos o sospechados también deben denunciarse a la policía y al Fiscal general del estado correspondiente. Este aviso no ha sido retrasado por las fuerzas policiales.

En el caso de los residentes del Distrito de Columbia, se podrá contactar al Fiscal General del Distrito de Columbia en: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; y oag@dc.gov.

En el caso de los residentes de Maryland, se podrá contactar al Fiscal general del estado de Maryland en: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 o 1-888-743-0023 y <https://www.marylandattorneygeneral.gov/>.

En el caso de los residentes de Nuevo México, los consumidores tienen derechos conforme a la Ley de Informe Crediticio Justo (Fair Credit Reporting Act, FCRA), como, por ejemplo, el derecho a que les digan si se utilizó la información en su archivo de crédito en contra de ellos, el derecho a saber lo que está en su archivo de crédito, el derecho a solicitar su calificación de crédito y el derecho a objetar la información incompleta o imprecisa. Asimismo, de conformidad con la Ley de Informe Crediticio Justo, las agencias de informes del consumidor deben corregir o suprimir toda información que sea imprecisa, esté incompleta o no se pueda verificar; las agencias de informes del consumidor no pueden reportar información negativa desactualizada; el acceso al archivo de los consumidores es limitado; los consumidores deben dar su consentimiento para que se entreguen los informes crediticios a los empleadores; los consumidores pueden limitar las ofertas “prefiltradas” de créditos y seguros que reciben en base a la información de su informe crediticio y los consumidores pueden solicitar compensación por daños y perjuicios de los infractores. Los consumidores podrían tener derechos adicionales en virtud de la Ley de Informe Crediticio Justo que no están resumidos en este documento. Las víctimas de robo de identidad y el personal de servicio militar activo tienen derechos adicionales específicos conforme a la Ley de Informe Crediticio Justo. Para revisar sus derechos conforme a la Ley de Informe Crediticio Justo, les recomendamos a los consumidores que visiten www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf o escriban a Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

En el caso de los residentes de Nueva York, se podrá contactar al fiscal general del estado de Nueva York en: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755 o <https://ag.ny.gov>.

En el caso de los residentes de Carolina del Norte, se podrá contactar al Fiscal general del estado de Carolina del Norte en: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 o 1-919-716-6000 y www.ncdoj.gov.

En el caso de los residentes de Rhode Island, se podrá contactar al fiscal general del estado de Rhode Island en: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov y 1-401-274-4400. En virtud de las leyes de Rhode Island, las personas tienen el derecho a obtener cualquier informe policial archivado respecto a este suceso. Hay aproximadamente 0 residentes de Rhode Island que pueden verse afectados por este evento.