

EXHIBIT 1

The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Texas Tech University Health Sciences Center El Paso (“TTUHSC EP”) does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about September 29, 2024, TTUHSC EP identified information technology issues that resulted in a temporary disruption to certain computer systems and applications. Immediately after identifying these issues, TTUHSC EP took steps to ensure the security of the TTUHSC EP network and began an investigation with the assistance of third-party specialists in order to determine the nature and scope of the incident. The investigation confirmed that a cybersecurity event caused the technology issues which involved the access to or removal of certain files and folders from TTUHSC EP systems between September 17, 2024 and September 29, 2024. As a result, TTUHSC EP conducted a detailed review of the systems that were involved in order to determine what information they may contain and to whom the information belongs. While ongoing, on or about December 17, 2024, TTUHSC EP completed a review that determined certain Washington resident information may be involved. While the information varies for each individual, the potentially impacted information includes name, Social Security number, medical record number, and/or diagnosis information.

Notice to Washington Residents

On or about November 25, 2024, TTUHSC EP posted notice of this incident on the TTUHSC EP website and distributed notice to relevant media outlets. On or about January 24, 2025, TTUHSC EP provided written notice of this incident to approximately eight hundred eighty-nine (889) Washington residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*. Notification to individuals is ongoing and TTUHSC EP may supplement this notification if it is determined that a significant number of additional Washington residents will receive notice.

Other Steps Taken and To Be Taken

Upon discovering the event, TTUHSC EP moved quickly to investigate and respond to the incident, assess the security of TTUHSC EP systems, and identify potentially affected individuals. Further, TTUHSC EP notified federal law enforcement and applicable regulators. TTUHSC EP is also working to implement additional safeguards to enhance system protection and monitoring and is reviewing relevant policies and procedures. TTUHSC EP is providing access to complimentary credit monitoring services for twelve (12) months, through IDX, to individuals whose information was potentially affected by this incident.


Additionally, TTUHSC EP is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including 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 health care and health insurance billing statements, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. TTUHSC EP is providing written notice of this incident to relevant state and federal regulators, as required.


EXHIBIT A


TTUHSC EL PASO
Texas Tech University Health Sciences Center El Paso
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>

January 24, 2025

NOTICE OF <<SECURITY INCIDENT/DATA BREACH>>

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

The Texas Tech University Health Sciences Center El Paso is writing to inform you of a recent incident which may impact your information. This notice provides you with details about the event, our response, and resources available to you to help protect your information from possible misuse, should you determine it is appropriate to do so.

What Happened? In September 2024, we identified issues that resulted in a temporary disruption to some computer systems and applications. Immediately after identifying these issues, we took steps to ensure the security of the network and began an investigation. The investigation subsequently confirmed a cybersecurity event caused the temporary disruption as well as access to or removal of certain files and folders from our network between September 17, 2024 and September 29, 2024. We then conducted a detailed review of the systems that were involved in order to determine what information they may contain and to whom it belongs.

What Information Was Involved? While the investigation is ongoing, on or about December 17, 2024 we completed a review that determined that your information was present in files which may be potentially affected by this incident. The potentially affected information may include your name and <<Variable Data - English>>. We are not aware of any actual or attempted identity theft or fraud in connection with this event.

What We Are Doing. The confidentiality, privacy, and security of information in our care is among our highest priorities. We are reviewing existing security policies and procedures as part of the investigation and are implementing additional safeguards to enhance system protection and monitoring.

Out of an abundance of caution, we are offering you access to complimentary credit monitoring and identity restoration assistance services for <<12/24>> months through IDX. A description of services and instructions regarding how to enroll can be found within the enclosed *Steps You Can Take to Help Protect Your Information*. Please note that you must complete the enrollment process yourself 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, to review account statements and monitor your credit reports, as well as health care and health insurance billing statements, for suspicious activity and to detect errors. In addition to enrolling in the credit monitoring services being offered to you, you may also review the information contained in the enclosed *Steps You Can Take to Help Protect Your Information* for more steps you can take, should you feel it is appropriate to do so.

For More Information. If you have further questions about this event, you can contact the toll-free dedicated assistance line at 1-866-902-1996, available Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

Texas Tech University Health Sciences Center El Paso

STEPS YOU CAN TAKE TO HELP PROTECT YOUR 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. Please note the deadline to enroll is April 24, 2025.

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 1-866-902-1996 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/credit-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 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

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their 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. Texas Tech University Health Sciences Center El Paso is located at 5001 El Paso Dr, El Paso, TX 79905.

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/>. Texas Tech University Health Sciences Center El Paso is located at 5001 El Paso Dr, El Paso, TX 79905.

For Massachusetts Residents, under Massachusetts law, you have the right to obtain a police report in regard to this event. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

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 59 Rhode Island residents that may be impacted by this event.

Código de inscripción: <<ENROLLMENT>>

Para inscribirse, escanee el código QR a continuación:



O visite:

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

24 de enero de 2025

AVISO DE <<INCIDENTE DE SEGURIDAD/FILTRACIÓN DE DATOS>>

Estimado/a <<First Name>> <<Last Name>>:

Texas Tech University Health Sciences Center El Paso le escribe para informarle de un incidente reciente que puede afectar su información. Este aviso le proporciona detalles sobre el evento, nuestra respuesta y los recursos a su disposición para ayudarle a proteger su información de un posible uso indebido, en caso de que lo considere oportuno.

¿Qué ocurrió? En septiembre de 2024, identificamos problemas que provocaron una interrupción temporal de algunos sistemas y aplicaciones informáticos. Inmediatamente después de identificar estos problemas, tomamos medidas para garantizar la seguridad de la red e iniciamos una investigación. La investigación confirmó posteriormente que, entre el 17 al 29 de septiembre de 2024, un evento de ciberseguridad causó la interrupción temporal, así como el acceso a determinados archivos y carpetas de nuestra red o su eliminación. Seguidamente, llevamos a cabo una revisión detallada de los sistemas implicados para determinar qué información pudieron contener y a quién pertenecía.

¿Qué información se vio involucrada? Si bien la investigación está en curso, el 17 de diciembre de 2024 o alrededor de esta fecha, completamos una revisión que determinó que su información estaba presente en archivos que pudieran estar potencialmente afectados por este incidente. La información potencialmente afectada pudiera incluir su nombre y <<Variable Data - Spanish>>. No conocemos ningún hecho o tentativa de robo de identidad o fraude relacionado con este suceso.

Qué estamos haciendo La confidencialidad, la privacidad y la seguridad de la información a nuestro cargo es una de nuestras mayores prioridades. Como parte de la investigación, estamos revisando las políticas y procedimientos de seguridad existentes y estamos aplicando salvaguardias adicionales para mejorar la protección y supervisión del sistema.

Como precaución adicional, también le ofrecemos acceso gratuito a de servicios de monitoreo de crédito y restauración de identidad gratuitos durante <<12/24>> meses a través de IDX. En el documento adjunto *Medidas que puede tomar para proteger su información* puede encontrar una descripción de los servicios e instrucciones sobre cómo inscribirse. Tenga en cuenta que debe completar el proceso de inscripción usted mismo, ya que no se nos permite inscribirlo en estos servicios en su nombre.

Lo que usted puede hacer. Le recomendamos que permanezca alerta ante los incidentes de robo de identidad y fraude, y que revise sus estados de cuenta y sus informes de crédito, así como los extractos de facturación de atención médica y del seguro médico, para detectar actividades sospechosas y errores. Además de inscribirse en los servicios de monitoreo de crédito que se le ofrecen, también puede consultar la información contenida en el documento adjunto *Medidas que puede tomar para proteger su información* para conocer otras medidas que puede tomar, si lo considera oportuno.

Para obtener más información. Si tiene más preguntas sobre este evento, puede comunicarse con la línea gratuita de asistencia dedicada a través del 1-866-902-1996, disponible de lunes a viernes de 8:00 a. m a 8:00 p. m., hora central, excluyendo los principales días festivos de EE. UU.

Atentamente,

Texas Tech University Health Sciences Center El Paso

MEDIDAS QUE PUEDE TOMAR PARA PROTEGER SU INFORMACIÓN PERSONAL

Inscríbese en los servicios de monitoreo

1. Sitio web e inscripción. Escanee la imagen QR o visite <https://app.idx.us/account-creation/protect> y siga las instrucciones de inscripción utilizando el código de inscripción que se le proporciona en la parte superior de la carta. Tenga en cuenta que la fecha límite para inscribirse es el 24 de abril de 2025.

2. Active el monitoreo de crédito proporcionado como parte de su membresía en la protección de identidad de IDX. El monitoreo incluido en la membresía debe estar activado para que funcione. Nota: Para poder utilizar este servicio debe tener un crédito establecido, y acceso a una computadora y a internet. Si necesita asistencia, IDX podrá ayudarlo.

3. Teléfono. Comuníquese con IDX a través del 1-866-902-1996 para obtener más información sobre este evento y hablar con representantes expertos sobre las medidas apropiadas que debe tomar para proteger su identidad crediticia.

Monitoree sus cuentas

Según la ley de los EE. UU., un consumidor tiene derecho a solicitar un informe de crédito gratuito por año de cada una de las tres principales agencias de informes de crédito: 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 también pueden comunicarse directamente con las tres principales agencias de informes de crédito que se enumeran a continuación para solicitar una copia gratuita de su informe crediticio.

Los consumidores tienen derecho a colocar una “alerta de fraude” inicial o extendida en un expediente de crédito, sin costo alguno. Una alerta de fraude inicial es una alerta que dura un año y que se incluye en el expediente de crédito del consumidor. Al ver una alerta de fraude en el expediente de crédito de un consumidor, una empresa está obligada a tomar medidas para verificar la identidad del consumidor antes de concederle un nuevo crédito. Si los consumidores son víctimas de robo de identidad, tienen derecho a una alerta de fraude extendida, que es una alerta de fraude de siete años de duración. Si los consumidores desean colocar una alerta de fraude, deben comunicarse con cualquiera de las tres principales agencias de informes de crédito que se enumeran a continuación.

Como alternativa a una alerta de fraude, los consumidores tienen derecho a colocar un “congelamiento de crédito” en un informe de crédito, lo que prohibirá que una agencia de crédito divulgue información en el informe de crédito sin la autorización expresa del consumidor. El congelamiento de crédito está diseñado para evitar que el crédito, los préstamos y los servicios se aprueben en nombre de un consumidor sin su consentimiento. Sin embargo, los consumidores deben saber que el uso de un congelamiento de crédito para controlar quién tiene acceso a la información personal y financiera en su informe crediticio puede retrasar, interferir o prohibir la aprobación oportuna de cualquier pedido o solicitud posterior que realicen con respecto a un nuevo préstamo, crédito, hipoteca, o cualquier otra cuenta que implique la concesión de un crédito. De conformidad con la ley federal, no se puede cobrar a los consumidores por colocar o levantar un congelamiento de crédito en su informe crediticio. Para solicitar un congelamiento de crédito, es posible que las personas deban proporcionar parte o la totalidad de la siguiente información:

1. Nombre completo (incluida la inicial del segundo nombre, así como Jr., Sr., III, etc.);
2. Número de Seguro Social;
3. Fecha de nacimiento;
4. Domicilios en los últimos dos a cinco años;
5. Comprobante de domicilio, como una factura actual de servicios públicos o de teléfono;
6. Fotocopia legible de una tarjeta de identificación emitida por el gobierno (licencia de conducir estatal o tarjeta de identificación estatal, etc.); y
7. Copia de la denuncia policial el informe de la investigación o la reclamación ante una agencia de orden público respecto del robo de identidad si es víctima de este delito.

Si los consumidores desean colocar un congelamiento de crédito o una de fraude, deben comunicarse con las tres principales agencias de informes de crédito que se enumeran a continuación:

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	1-833-799-5355
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

Información adicional

Los consumidores pueden informarse aún más sobre el robo de identidad, las alertas de fraude, los congelamientos de crédito y las medidas que pueden tomar para proteger su información personal comunicándose con las agencias de informes del consumidor, la Comisión Federal de Comercio o el Fiscal General de su estado. Puede comunicarse con la Comisión Federal de Comercio en: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); y TTY: 1-866-653-4261. La Comisión Federal de Comercio también recomienda a quienes descubran que se ha hecho un uso indebido de su información que presenten una reclamación ante ellos. Los consumidores pueden obtener más información sobre cómo presentar dicha reclamación a través de la información de contacto mencionada anteriormente. Los consumidores tienen derecho a presentar una denuncia policial si alguna vez sufren un robo de identidad o un fraude. Tenga en cuenta que, para presentar una denuncia ante las autoridades policiales por robo de identidad, es probable que los consumidores deban proporcionar alguna prueba de que han sido víctimas. Los casos de robo de identidad conocido o presuntos también deben informarse a las autoridades policiales y al fiscal general del estado correspondiente. Las autoridades policiales no han aplazado este aviso.

Los residentes del Distrito de Columbia pueden comunicarse con el fiscal general del Distrito de Columbia en: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; y oag.dc.gov. Texas Tech University Health Sciences Center El Paso se encuentra en 5001 El Paso Dr, El Paso, TX 79905.

Los residentes de Maryland pueden comunicarse con el fiscal general 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/>. Texas Tech University Health Sciences Center El Paso se encuentra en 5001 El Paso Dr, El Paso, TX 79905.

Los residentes de Massachusetts, conforme a la ley de Massachusetts, tienen derecho a presentar una denuncia policial respecto a este evento. Si es víctima de un robo de identidad, también tiene derecho a presentar una denuncia policial y obtener una copia de ella.

Para los residentes de Nuevo México, los consumidores tienen derechos de conformidad con la Ley de Informes de Crédito Justos, como el derecho a que se les informe si los datos de su expediente de crédito se ha utilizado en su contra, el derecho a saber qué figura en su expediente de crédito, el derecho a solicitar su calificación crediticia y el derecho a objetar información incompleta o inexacta. Además, de conformidad con la Ley de Informes de Crédito Justos, las agencias de informes de los consumidores deben corregir o eliminar información inexacta, incompleta o no verificable; las agencias de informes de los consumidores no pueden reportar información negativa obsoleta; el acceso a los expedientes de los consumidores es limitado; los consumidores deben dar su consentimiento para que se proporcionen informes de crédito a los empleadores; los consumidores pueden limitar las ofertas de crédito y de seguro "preseleccionadas" basadas en la información de su informe de crédito; y los consumidores pueden solicitar daños y perjuicios a los infractores. Los consumidores pueden tener derechos adicionales conforme a la Ley de Informes de Crédito Justos, que no figuran aquí. Las víctimas del robo de identidad y el personal militar en servicio activo tienen derechos adicionales específicos conforme a la Ley de Informes de Crédito Justos. Le recomendamos que consulte sus derechos conforme a la Ley de Informes de Crédito Justos visitando www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, o escribiendo a Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Los residentes de Nueva York pueden comunicarse con el fiscal general de Nueva York en Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

Los residentes de Carolina del Norte pueden comunicarse con el fiscal general 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.

Los residentes de Rhode Island pueden comunicarse con el fiscal general de Rhode Island en: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Según la ley de Rhode Island, las personas tienen derecho a obtener cualquier informe policial presentado con respecto a este evento. Existen aproximadamente 59 residentes de Rhode Island que pueden verse afectados por este evento.