

August 6, 2024

Paul Connell

+1 202 663 6067 (t)
+1 202 663 6363 (f)
paul.connell@wilmerhale.com

Via E-Mail to Idtheft@oag.state.md.us

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Breach Notification

To Whom It May Concern:

I am writing on behalf of my client Change Healthcare Inc. (“CHC”), a subsidiary of UnitedHealth Group Incorporated (“UHG”), to inform you of a security incident. While the data breach notification law in your state generally does not require notice where the reporting company makes notifications in compliance with other applicable federal data breach reporting requirements, CHC is providing this notice as a courtesy given that the incident may have involved the protected health information (PHI) or personally identifiable information (PII) of residents in your state.

CHC provides products and services in the healthcare space to support payors, providers, third-party administrators, pharmacies, and other partners. It operates as a business associate under the Health Insurance Portability and Accountability Act (HIPAA) as part of offering its services to its customers.

What Happened

On February 21, 2024, CHC became aware of deployment of ransomware in its computer system. Once discovered, CHC quickly took steps to stop the activity, disconnected and turned off systems to prevent further impact, began an investigation, and contacted law enforcement. CHC’s security team worked around the clock with several top security experts to address the matter and understand what happened. CHC has not identified evidence this incident spread beyond CHC.

Who Was Impacted

Assisted by leading experts, CHC has been analyzing its data and systems to determine which customers’ and individuals’ data were impacted by the incident. At this time, CHC is in the late stages of identifying specific covered entities and specific individuals impacted by this incident. Although data review is not yet complete, and additional impacted customers and individuals may be identified, on June 20, 2024, CHC began providing notice to identified impacted customers whose members’ or patients’ data was involved in the incident. CHC is assuming responsibility

August 6, 2024

Page 2

for making individual notifications on behalf of those impacted customers unless such customers opt out of CHC's individual notification process.

CHC's notice to customers also included a mechanism for those customers to provide substitute notice to their potentially impacted individuals in a manner consistent with HIPAA. CHC and UHG have also made this substitute notice available through their websites.

CHC plans to send direct notice (written letters) to affected individuals at the conclusion of the data review where CHC has a sufficient address, unless a customer has opted out of CHC providing notice to individuals on its behalf. To the extent that an affected individual's PHI was impacted and they cannot be attributed to a CHC customer, those individuals will also receive a letter so long as CHC has a sufficient address for them. The mailing process began in late July.

What Information Was Impacted

While CHC cannot confirm exactly what data has been affected for each specific individual, based on its review to date, the data that may have been seen and taken may include contact information (such as name, address, date of birth, phone number, and email) plus one or more of the following:

- Health insurance data (such as health plans/policies, insurance companies, member/group ID numbers, and Medicaid-Medicare-government payor ID numbers)
- Health data (such as medical record numbers, doctors, diagnoses, medicines, test results, images, care, and treatment)
- Billing, insurance claims and payment data (such as claim numbers, account numbers, billing codes, payment cards, financial and banking, and balance)
- Other personal data (such as Social Security number, driver's license or state ID number, or other ID number)

The data that may have been seen and taken was not the same for everyone. Some of this data may be about the person who paid the bill for health care services.

What CHC Is Doing

In response to this incident, CHC immediately took action to shut down systems and sever connectivity to prevent further impact. CHC worked around the clock from the day of the ransomware deployment and has devoted significant resources to the response and restoration efforts, as well as retained several expert forensic firms to analyze the impacted data. CHC has also reinforced its policies and practices and implemented additional safeguards in an effort to

August 6, 2024

Page 3

prevent similar incidents from occurring in the future. CHC, along with leading external industry experts, continues to monitor the internet and dark web to determine if data has been published.

Rather than waiting for the completion of the data review, on April 22, 2024, CHC began providing free credit monitoring and identity theft protection services for two years to any U.S. individual who is concerned they may have been impacted, along with a dedicated call center staffed by clinicians to provide additional support services. Individuals may also visit changeCyberSupport.com for more information about the incident.

* * *

WilmerHale has designated this letter as confidential because it contains confidential and proprietary business information that is exempt from a request under the Maryland Public Information Act ("MD PIA"). *See* Md. Ann. Code art. GP, § 4-101 *et seq.* We request that you take all available steps to prevent the disclosure of this letter to third parties.

We assert all available protections regarding this information so that it will not be released without CHC's written authorization.

CHC does not intend to, and does not, waive any applicable privilege. If it were found that any of the information provided constitutes disclosure of otherwise privileged matters such disclosure would be inadvertent.

Please do not hesitate to contact me if you have any questions.

Best regards,

Paul Connell

Paul Connell

[INSERT CHC NAME AND LOGO]

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



Location of 2D Barcode
(X=80.0 mm, Y=39.50 mm)

July 29, 2024

<<First Name>><<Middle Initial>><<Last Name>><<Suffix>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>

Notice of Data Breach

To <<First Name>> <<Middle Initial>> <<Last Name>> <<Suffix>>:

We are sorry to tell you about a privacy event. This letter is from Change Healthcare (“CHC”). We work with many doctors, health insurance plans, and other health companies to help provide health services or benefits. This event may have involved your data.

What happened?

On February 21, 2024, CHC found activity in our computer system that happened without our permission. We quickly took steps to stop that activity. We began investigating right away, and hired a special team to help us. We also called law enforcement. We also turned off CHC’s systems to help protect our customers and their individuals.

On March 7, 2024, we learned a cybercriminal was able to see and take copies of some data in our computer system. This happened between February 17, 2024 and February 20, 2024. We received files that were safe to look at on March 13, 2024.

What information was involved?

We have told our clients about this event. Starting on June 20, 2024, we also told our clients about what data may have been seen and taken. We encourage you to remain vigilant by checking bills and accounts. The data that may have been seen and taken includes contact information (such as name, address, date of birth, phone number, and email) plus one or more of the following:

- Health insurance data (such as health plans/policies, insurance companies, member/group ID numbers, and Medicaid-Medicare-government payor ID numbers)
- Health data (such as medical record numbers, doctors, diagnoses, medicines, test results, images, care, and treatment)
- Billing, insurance claims and payment data (such as claim numbers, account numbers, billing codes, payment cards, financial and banking, and balance)
- Other personal data (such as Social Security number, driver’s license or state ID number, or other ID number)

The data that may have been seen and taken was not the same for everyone. Some of this data may be about the person who paid the bill for health care services.

[PwC GUID placeholder]

Why did this happen?

A cybercriminal accessed our computer system without our permission.

What is CHC doing?

We investigated and called law enforcement. We are also making our computer systems even stronger than before. We do not want this to happen again.

We would like to offer you free credit monitoring and identity theft protection services. We will pay for the cost of this service for 2 years so that it is free for you. We have attached steps on how to sign up for this free service.

What you can do:

You can sign up for the free credit monitoring and identity protection services. Be sure that bills and accounts look correct. We have attached steps on how to do that. If you learn of a crime against you, you can file a report with law enforcement.

What if I have a question?

If you have any questions or concerns, please call us toll free at 1-866-262-5342. You can also learn more at changeybersupport.com. We are sorry for any concern this event may cause.

Sincerely,

Change Healthcare Privacy Office

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



Location of 2D Barcode
(X=80.0 mm, Y=39.50 mm)

July 29, 2024

<<First Name>><<Middle Initial>><<Last Name>><<Suffix>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>

Aviso de filtración de datos

Para<<First Name>> <<Middle Initial>> <<Last Name>> <<Suffix>>:

Lamentamos informarle sobre una filtración de datos . Esta carta es de Change Healthcare ("CHC"). Trabajamos con muchos médicos, planes de seguro médico y otras compañías de salud para brindar servicios o beneficios de salud. Este evento puede haber involucrado sus datos.

¿Qué sucedió?

El 21 de febrero de 2024, CHC detectó que hubo actividad en nuestro sistema informático sin nuestro permiso. Rápidamente tomamos medidas para detener dicha actividad. Comenzamos a investigar de inmediato y contratamos a un equipo especial para que nos ayudara. También llamamos a la policía. Asimismo, desactivamos los sistemas de CHC para proteger a nuestros clientes y a sus personas.

El 7 de marzo de 2024, nos enteramos de que un ciberdelincuente pudo ver y tomar copias de algunos datos en nuestro sistema informático. Esto sucedió entre el 17 de febrero de 2024 y el 20 de febrero de 2024. Recibimos archivos que eran seguros para consultar el 13 de marzo de 2024.

¿Qué información se vio involucrada?

Les informamos a nuestros clientes sobre este evento. A partir del 20 de junio de 2024, también informamos a nuestros clientes sobre qué datos pudieron haberse visto y extraído. Le recomendamos que permanezca alerta revisando las facturas y cuentas. Los datos que se pudieron haber visto y extraído incluyen información de contacto (como nombre, dirección, fecha de nacimiento, número de teléfono y correo electrónico) y uno o más de los siguientes detalles:

- Datos del seguro médico (como planes/pólizas de salud, compañías de seguros, números de identificación de miembros/grupos y números de identificación de pagadores del gobierno de Medicaid-Medicare)
- Datos de salud (como números de historias clínicas, médicos, diagnósticos, medicamentos, resultados de pruebas, imágenes, atención y tratamiento)
- Facturación, reclamaciones de seguros y datos de pago (como números de reclamación, números de cuenta, códigos de facturación, tarjetas de pago, datos financieros y bancarios, y saldo)
- Otros datos personales (como el número de Seguro Social, la licencia de conducir o el número de identificación estatal, u otro número de identificación)

Los datos que se pudieron haber visto y extraído no eran los mismos para todos. Algunos de estos datos pueden ser sobre la persona que pagó la factura de los servicios de atención médica.

¿Por qué ocurrió esto?

Un ciberdelincuente accedió a nuestro sistema informático sin nuestro permiso.

¿Qué está haciendo CHC?

Investigamos y llamamos a la policía. También estamos reforzando nuestros sistemas informáticos aún más que antes. No queremos que esto vuelva a suceder.

Nos gustaría ofrecerle servicios gratuitos de monitoreo de crédito y protección contra el robo de identidad. Pagaremos el costo de este servicio durante 2 años para que sea gratis para usted. Hemos adjuntado los pasos a seguir para registrarse en este servicio gratuito.

Qué puede hacer usted:

Puede suscribirse a los servicios gratuitos de monitoreo de crédito y protección de identidad. Verifique que las facturas y las cuentas sean correctas. Se adjuntan los pasos sobre cómo hacerlo. Si se entera de un delito en su contra, puede presentar una denuncia ante la policía.

¿Y si tengo una pregunta?

Si tiene alguna pregunta o inquietud, llámenos al número gratuito 1-866-262-5342. También puede obtener más información en changeybersupport.com. Lamentamos cualquier preocupación que este evento pueda causar.

Atentamente.

Change Healthcare Privacy Office

ATTENTION: If you speak English, language assistance services, free of charge, are available to you. Call 1-866-262-5342 (TTY: 1-866-262-5342).

ATENCIÓN: si habla español, tiene a su disposición servicios gratuitos de asistencia lingüística. Llame al 1-866-262-5342 (TTY: 1-866-262-5342).

ATANSYON: Si w pale Kreyòl Ayisyen, gen sèvis èd pou lang ki disponib gratis pou ou. Rele 1-866-262-5342 (TTY: 1-866-262-5342)

CHÚ Ý: Nếu bạn nói Tiếng Việt, có các dịch vụ hỗ trợ ngôn ngữ miễn phí dành cho bạn. Gọi số 1-866-262-5342 (TTY: 1-866-262-5342).

ATENÇÃO: Se fala português, encontram-se disponíveis serviços linguísticos, grátis. Ligue para 1-866-262-5342 (TTY: 1-866-262-5342).

注意:如果您使用繁體中文, 您可以免費獲得語言援助服務。請致電 1-866-262-5342 (TTY: 1-866-262-5342)。

ATTENTION : Si vous parlez français, des services d'aide linguistique vous sont proposés gratuitement. Appelez le 1-866-262-5342 (ATS : 1-866-262-5342).

PAUNAWA: Kung nagsasalita ka ng Tagalog, maaari kang gumamit ng mga serbisyo ng tulong sa wika nang walang bayad. Tumawag sa 1-866-262-5342 (TTY: 1-866-262-5342).

ВНИМАНИЕ: Если вы говорите на русском языке, то вам доступны бесплатные услуги перевода. Звоните 1-866-262-5342 (телетайп: 1-866-262-5342).

ملحوظة: إذا كنت تتحدث اذكر اللغة، فإن خدمات المساعدة اللغوية تتوافر لك بالمجان. اتصل برقم 1-866-262-5342 (رقم هاتف الصم والبكم: 1-866-262-5342).

ATTENZIONE: In cask la lingua palatal said litigant, so no disponibili servizi di assistenza linguistica gratuiti. Chiamare il numero 1-866-262-5342 (TTY: 1-866-262-5342).

ACHTUNG: Wenn Sie Deutsch sprechen, stehen Ihnen kostenlos sprachliche Hilfsdienstleistungen zur Verfügung. Rufnummer: 1-866-262-5342 (TTY: 1-866-262-5342).

주의: 한국어를 사용하시는 경우, 언어 지원 서비스를 무료로 이용하실 수 있습니다. 1-866-262-5342 (TTY: 1-866-262-5342)번으로 전화해 주십시오.

UWAGA: Jeżeli mówisz po polsku, możesz skorzystać z bezpłatnej pomocy językowej. Zadzwoń pod numer 1-866-262-5342 (TTY: 1-866-262-5342).

સુચના: જો તમે ગુજરાતી બોલતા હો, તો નિ:શુલ્ક ભાષા સહાય સેવાઓ તમારા માટે ઉપલબ્ધ છે. ફોન કરો 1-866-262-5342 (TTY: 1-866-262-5342).

เรียน :ถ้า คุณพูด ภาษาไทยคุณสามารถใช้ บริการช่วยเหลือทางภาษาได้ฟรี โทร 1-866-262-5342 (TTY: 1-866-262-5342).

REFERENCE GUIDE

Review Your Account Statements

Carefully review statements sent to you from your healthcare providers, insurance company, and financial institutions to ensure that all of your account activity is valid. Report any questionable charges promptly to the provider or company with which you maintain the account.

Provide Any Updated Personal Information to Your Health Care Provider

Your health care provider's office may ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office may also ask you to confirm your date of birth, address, telephone, and other pertinent information so that they can make sure that all of your information is up-to-date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit can help to avoid problems and to address them quickly should there be any discrepancies.

Order Your Free Credit Report

To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

How to Enroll in IDX Credit and Identity Monitoring Services

As a safeguard, you may enroll, at no cost to you, in online credit monitoring and identity restoration services provided by IDX for two years. To enroll in these services, please call CHC at 1-866-262-5342 and ask to enroll.

Individuals must enroll in order for the available services to go into effect, and the monitoring included in the membership must be activated to be effective. Please note that credit monitoring services may not be available for individuals who have not established credit or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score. If you need assistance, IDX will be able to assist you.

We encourage you to take advantage of these protections and remain vigilant for incidents of potential fraud and identity theft, including regularly reviewing and monitoring your credit reports and account statements.

Contact the U.S. Federal Trade Commission

If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidents of identity theft or fraud, promptly report the matter to your local law enforcement authorities, state Attorney General and the FTC.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the following contact information: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.ftc.gov/idtheft/.

Place a Fraud Alert on Your Credit File

To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect against the possibility of an identity thief opening new credit accounts in your name. When a credit grantor checks the credit history of someone applying for credit, the credit grantor gets a notice that the applicant may be the victim of identity theft. The alert notifies the credit grantor to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows flagging of your file with a fraud alert at all three credit bureaus.

Equifax	P.O. Box 105069 Atlanta, Georgia 30348	1- 888-766-0008	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

Security Freezes

You have the right to request a credit freeze from a consumer reporting agency, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit bureau. To place a security freeze on your credit report you must contact the credit reporting agency by phone, mail, or secure electronic means and provide proper identification of your identity. The following information must be included when requesting a security freeze (note that if you are requesting a security freeze for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

Below, please find relevant contact information for the three consumer reporting agencies:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	1-800-685-1111	www.equifax.com
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	1-888-909-8872	www.transunion.com

Once you have submitted your request, the credit reporting agency must place the security freeze no later than 1 business day after receiving a request by phone or secure electronic means, and no later than 3 business days

after receiving a request by mail. No later than five business days after placing the security freeze, the credit reporting agency will send you confirmation and information on how you can remove the freeze in the future.

For Residents Of	Additional Information
District of Columbia	You may contact the D.C. Attorney General's Office to obtain information about steps to take to avoid identity theft: D.C. Attorney General's Office, Office of Consumer Protection, 400 6th Street, NW, Washington DC 20001, 1-202-442-9828, www.oag.dc.gov .
Iowa	You may contact law enforcement or the Iowa Attorney General's office to report suspected incidents of identity theft. The Iowa Attorney General's Office can be reached at: Iowa Attorney General's Office, Director of Consumer Protection Division, 1305 E. Walnut Street, Des Moines, IA 50319, 1-515-281-5926, www.iowattorneygeneral.gov .
Maryland	You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, http://www.marylandattorneygeneral.gov/ .
Massachusetts	You have the right to obtain a police report with respect to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.
New Mexico	New Mexico consumers have the right to obtain a security freeze or submit a declaration of removal. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following: (1) the unique personal identification number, password or similar device provided by the consumer reporting agency; (2) proper identification to verify your identity; and (3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report. A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone. A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act. If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before

	you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.
New York	You may also obtain information about security breach response and identity theft prevention and protection from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, www.ag.ny.gov.
North Carolina	You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6000, www.ncdoj.gov.
Oregon	State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. Contact information for the Oregon Department of Justice is as follows: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301, 1-877-877-9392, www.doj.state.or.us.
Rhode Island	You have a right to file or obtain a police report related to this incident. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Office of the Attorney General, 150 South Main Street, Providence, RI, 02903, 1-401-274-4400, www.riag.ri.gov.

ATTENTION: If you speak English, language assistance services, free of charge, are available to you. Call 1-866-262-5342 (TTY: 1-866-262-5342).

ATENCIÓN: si habla español, tiene a su disposición servicios gratuitos de asistencia lingüística. Llame al 1-866-262-5342 (TTY: 1-866-262-5342).

ATANSYON: Si w pale Kreyòl Ayisyen, gen sèvis èd pou lang ki disponib gratis pou ou. Rele 1-866-262-5342 (TTY: 1-866-262-5342)

CHÚ Ý: Nếu bạn nói Tiếng Việt, có các dịch vụ hỗ trợ ngôn ngữ miễn phí dành cho bạn. Gọi số 1-866-262-5342 (TTY: 1-866-262-5342).

ATENÇÃO: Se fala português, encontram-se disponíveis serviços linguísticos, grátis. Ligue para 1-866-262-5342 (TTY: 1-866-262-5342).

注意:如果您使用繁體中文, 您可以免費獲得語言援助服務。請致電 1-866-262-5342 (TTY: 1-866-262-5342)。

ATTENTION : Si vous parlez français, des services d'aide linguistique vous sont proposés gratuitement. Appelez le 1-866-262-5342 (ATS : 1-866-262-5342).

PAUNAWA: Kung nagsasalita ka ng Tagalog, maaari kang gumamit ng mga serbisyo ng tulong sa wika nang walang bayad. Tumawag sa 1-866-262-5342 (TTY: 1-866-262-5342).

ВНИМАНИЕ: Если вы говорите на русском языке, то вам доступны бесплатные услуги перевода. Звоните 1-866-262-5342 (телетайп: 1-866-262-5342).

ملحوظة: إذا كنت تتحدث اذكر اللغة، فإن خدمات المساعدة اللغوية تتوافر لك بالمجان. اتصل برقم 1-866-262-5342 (رقم هاتف

الصم والبكم: 1-866-262-5342).

ATTENZIONE: In cask la lingua palatal said litigant, so no disponibili servizi di assistenza linguistica gratuiti. Chiamare il numero 1-866-262-5342 (TTY: 1-866-262-5342).

ACHTUNG: Wenn Sie Deutsch sprechen, stehen Ihnen kostenlos sprachliche Hilfsdienstleistungen zur Verfügung. Rufnummer: 1-866-262-5342 (TTY: 1-866-262-5342).

주의: 한국어를 사용하시는 경우, 언어 지원 서비스를 무료로 이용하실 수 있습니다. 1-866-262-5342 (TTY: 1-866-262-5342)번으로 전화해 주십시오.

UWAGA: Jeżeli mówisz po polsku, możesz skorzystać z bezpłatnej pomocy językowej. Zadzwoń pod numer 1-866-262-5342 (TTY: 1-866-262-5342).

સુચના: જો તમે ગુજરાતી બોલતા હો, તો નિઃશુલ્ક ભાષા સહાય સેવાઓ તમારા માટે ઉપલબ્ધ છે. ફોન કરો 1-866-262-5342 (TTY: 1-866-262-5342).

เรียน :ถ้า คุณพูด ภาษาไทยคุณสามารถใช้บริการช่วยเหลือทางภาษาได้ฟรี โทร 1-866-262-5342 (TTY: 1-866-262-5342).

GUÍA DE REFERENCIA

Revise sus estados de cuenta

Revise cuidadosamente los estados de cuenta que recibe de sus proveedores de atención médica, compañía de seguro e instituciones financieras para asegurarse de que toda la actividad de su cuenta sea válida. Informe cualquier cargo cuestionable de inmediato a la empresa con la que mantiene la cuenta.

Proporcione cualquier información personal actualizada a su proveedor de atención médica

El consultorio de su proveedor de atención médica puede solicitar ver una identificación con fotografía para verificar su identidad. Lleve una identificación con fotografía a cada cita si es posible. El consultorio de su proveedor también puede pedirle que confirme su fecha de nacimiento, dirección, teléfono y otra información pertinente para asegurarse de que toda su información esté actualizada. Asegúrese de informar al consultorio de su proveedor cuando haya algún cambio en su información. Revisar cuidadosamente esta información con el consultorio de su proveedor en cada visita puede ayudar a evitar problemas y abordarlos rápidamente en caso de alguna discrepancia.

Solicite su informe de crédito gratuito

Para solicitar su informe de crédito anual gratuito, visite www.annualcreditreport.com, llame al número gratuito (877) 322-8228, o complete el Formulario de Solicitud de Informe de Crédito Anual en el sitio web de la Comisión Federal de Comercio (FTC) en www.ftc.gov y envíelo por correo a Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Las tres agencias de crédito entregan informes crediticios anuales sin costo solo a través del sitio web, del número de teléfono gratuito o del formulario de solicitud.

Al recibir su informe de crédito, revíselo cuidadosamente. Busque cuentas que no haya abierto. Busque en la sección de “inquiries” (consultas) los nombres de los acreedores a los que no ha solicitado crédito. Algunas empresas facturan con nombres distintos al de la tienda o nombre comercial; las agencias de crédito podrán informarle si este es el caso. Busque en la sección de “personal information” (información personal) cualquier inexactitud en la información (como su dirección postal y el número de Seguro Social).

Si ve algo que no entiende, llame a la agencia de crédito al número de teléfono que figura en el informe. Los errores pueden ser una señal de advertencia de un posible robo de identidad. Debe notificar a las agencias de crédito sobre cualquier inexactitud en su informe, ya sea por error o fraude, tan pronto como sea posible para que la información pueda ser investigada y, si se encuentra que está errónea, ser corregida. Si hay cuentas o cargos que usted no autorizó, notifique inmediatamente a la agencia de crédito correspondiente por teléfono y por escrito. La información que no se pueda explicar también debe informarse a la policía local o a la oficina del alguacil porque puede indicar alguna actividad delictiva.

Cómo inscribirse en los servicios de monitoreo de identidad y crédito de IDX

Como garantía, puede inscribirse, sin costo alguno para usted, en los servicios de monitoreo de crédito y restauración de identidad en línea que IDX le brinda por dos años. Para inscribirse en estos servicios, llame a CHC al 1-866-262-5342 y solicite inscribirse.

Las personas deben inscribirse para que los servicios disponibles entren en vigencia, y el monitoreo incluido en la membresía debe activarse para que sea efectivo. Tenga en cuenta que es posible que los servicios de monitoreo de crédito no estén disponibles para las personas que no tienen un expediente de crédito o una dirección en los Estados Unidos (o sus territorios) y un número de Seguro Social válido. Inscribirse en este servicio no afectará su calificación crediticia. Si necesita ayuda, IDX podrá brindarle asistencia.

Le recomendamos que aproveche estas protecciones y se mantenga alerta ante incidentes de posible fraude y robo de identidad, incluida la revisión y el control regulares de sus informes de crédito y estados de cuenta.

Comuníquese con la Comisión Federal de Comercio de los EE. UU.

Si detecta transacciones no autorizadas en cualquiera de sus cuentas financieras, notifique de inmediato a la compañía de tarjetas de pago o institución financiera correspondiente. Si detecta algún incidente de robo de identidad o fraude, informe de inmediato el asunto a las autoridades policiales locales, al Fiscal General del estado y a la FTC.

Puede comunicarse con la FTC para obtener más información sobre cómo protegerse de ser víctima de robo de identidad utilizando la siguiente información de contacto: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.ftc.gov/idtheft/.

Coloque una alerta de fraude en su informe de crédito

Para protegerse de un posible robo de identidad, considere colocar una alerta de fraude en su informe de crédito. Una alerta de fraude ayuda a protegerse contra la posibilidad de que un delincuente abra nuevas cuentas de crédito a su nombre. Cuando un otorgante de crédito verifica el historial de crédito de un solicitante, recibe un aviso de que el solicitante puede ser víctima de robo de identidad. La alerta notifica al otorgante del crédito para que tome medidas y verifique la identidad del solicitante. Puede colocar una alerta de fraude en su informe de crédito llamando a cualquiera de los números gratuitos de prevención de fraude que se proporcionan a continuación. Lo atenderá un sistema telefónico automatizado que permite marcar su informe con una alerta de fraude en las tres agencias de crédito.

Equifax	P.O. Box 105069 Atlanta, Georgia 30348	1- 888-766-0008	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

Congelamiento de seguridad

Usted tiene derecho a solicitar un congelamiento de crédito de una agencia de informes del consumidor, sin cargo, para que no sea posible abrir un nuevo crédito a su nombre sin el uso de un número PIN que se le entrega cuando inicia un congelamiento. Un congelamiento de seguridad está diseñado para evitar que posibles acreedores accedan a su informe de crédito sin su consentimiento. Si coloca un congelamiento de seguridad, los acreedores potenciales y otros terceros no podrán acceder a su informe de crédito a menos que levante temporalmente el congelamiento. En consecuencia, el uso de un congelamiento de seguridad puede retrasar su capacidad para obtener crédito.

A diferencia de una alerta de fraude, debe colocar un congelamiento de seguridad en su informe de crédito por separado en cada agencia de informes de crédito. Para colocar un congelamiento de seguridad en su informe de crédito, debe comunicarse con la agencia por teléfono, correo postal o algún medio electrónico seguro y proporcionar una identificación. Al solicitar un congelamiento de seguridad se debe incluir la siguiente información (tenga en cuenta que si está solicitando un informe de crédito para su cónyuge, esta información debe ser proporcionada por él/ella también): (1) nombre completo, con la inicial del segundo nombre y cualquier sufijo; (2) número de Seguro Social; (3) fecha de nacimiento; (4) dirección actual y cualquier dirección anterior durante los últimos cinco años; y (5) cualquier informe de incidente o queja pertinente ante una agencia de orden público o ante el Registro de Vehículos Motorizados. La solicitud también debe incluir una copia de una tarjeta de identificación emitida por el gobierno y una copia de una factura de servicios públicos reciente o un estado de cuenta bancario o de seguro. Es esencial que cada copia sea legible, muestre su nombre y dirección postal actual, y la fecha de emisión.

A continuación, encontrará información de contacto relevante para las tres agencias de informes del consumidor:

Equifax Security Freeze	P.O. Box 105788 Atlanta, GA 30348	1-800-685-1111	www.equifax.com
Experian Security Freeze	P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	P.O. Box 160 Woodlyn, PA 19094	1-888-909-8872	www.transunion.com

Una vez que haya enviado su solicitud, la agencia de informes de crédito debe colocar el congelamiento de seguridad a más tardar 1 día hábil después de recibir una solicitud por teléfono o medio electrónico seguro, y a más tardar 3 días hábiles después de recibir una solicitud por correo postal. A más tardar cinco días hábiles después de colocar el congelamiento de seguridad, la agencia de informes crediticios le enviará confirmación e información sobre cómo puede eliminar el congelamiento en el futuro.

Para residentes de	Información adicional
Distrito de Columbia	Puede comunicarse con la Oficina del Fiscal General de D.C. para obtener información sobre las medidas a tomar en función de evitar el robo de identidad: Attorney General's Office, Office of Consumer Protection, 400 6th Street, NW, Washington DC 20001, 1-202-442-9828, www.oag.dc.gov .
Iowa	Se puede comunicar con las autoridades policiales y judiciales o con la oficina del Fiscal General de Iowa para denunciar presuntos incidentes de robo de identidad. Puede comunicarse con la Oficina del Fiscal General de Iowa en: Iowa Attorney General's Office, Director of Consumer Protection Division, 1305 E. Walnut Street, Des Moines, IA 50319, 1-515-281-5926, www.iowattorneygeneral.gov .
Maryland	También puede obtener información sobre cómo prevenir y evitar el robo de identidad, en la Oficina del Fiscal General de Maryland: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, http://www.marylandattorneygeneral.gov/ .
Massachusetts	Tiene derecho a obtener una denuncia policial con respecto a este incidente. Si es víctima de un robo de identidad, también tiene derecho a presentar una denuncia policial y obtener una copia de ella.
Nuevo México	Los consumidores de Nuevo México tienen derecho a obtener un congelamiento de seguridad o presentar una declaración de remoción. Usted puede obtener un congelamiento de seguridad en su informe de crédito para proteger su privacidad y asegurarse de que no se otorgue crédito en su nombre sin su conocimiento. Puede presentar una declaración de remoción para eliminar la información que aparezca en su informe de crédito como resultado de ser víctima de robo de identidad. Usted tiene derecho a colocar un congelamiento de seguridad en su informe de crédito o presentar una declaración de remoción de conformidad con la Ley de Informes de Crédito Justos y Seguridad de la Identidad. El congelamiento de seguridad prohibirá que una agencia de informes del consumidor divulgue cualquier información en su informe de crédito sin su autorización o aprobación expresa. El congelamiento de seguridad está diseñado para prevenir que se aprueben créditos, préstamos y servicios en su nombre sin su consentimiento. Cuando coloque un congelamiento de seguridad en su informe de crédito, se le proporcionará un número de identificación personal, contraseña o dispositivo similar para usar en caso de que elija eliminar el congelamiento en su informe de crédito o autorizar temporalmente su divulgación a una parte o partes específicas o por un período de tiempo específico una vez

	que el congelamiento esté activo. Para eliminar el congelamiento o proporcionar autorización para divulgar temporalmente su informe de crédito, debe comunicarse con la agencia de informes del consumidor y proporcionar todo lo siguiente: (1) el número de identificación personal único, contraseña o dispositivo similar proporcionado por la agencia de informes del consumidor; (2) identificación adecuada para verificar su identidad; y (3) información sobre el tercero o terceros que recibirán el informe de crédito o el período de tiempo durante el cual el informe de crédito puede ser divulgado a los usuarios del mismo. Una agencia de información al consumidor que reciba una solicitud de un consumidor para levantar temporalmente un congelamiento en un informe de crédito deberá cumplir con la solicitud a más tardar tres días hábiles después de recibir la solicitud. A partir del 1.º de septiembre de 2008, las agencias de informes del consumidor deberán cumplir con la solicitud dentro de los quince minutos posteriores a la recepción de la solicitud por un método electrónico seguro o por teléfono. Un congelamiento de seguridad no se aplica en todas las circunstancias, como cuando usted tiene una relación de cuenta activa y su acreedor o sus agentes solicitan una copia de su informe de crédito para ciertos tipos de revisión de cuentas, cobro, control de fraude o actividades similares; para el establecimiento o ajuste de una tasa de seguro o reclamo o suscripción de seguro; para ciertos fines gubernamentales; y para fines de preselección como se define en la Ley Federal de Informes de Crédito Justos. Si está buscando obtener un nuevo crédito, préstamo, servicio público, teléfono o cuenta de seguro, debe entender que los procedimientos involucrados en el levantamiento de un congelamiento de seguridad pueden ralentizar sus solicitudes de crédito. Debe planificar y levantar un congelamiento con suficiente antelación, ya sea completamente si está comprando o específicamente para un determinado acreedor, antes de solicitar un nuevo crédito para que el levantamiento surta efecto. Debe comunicarse con una agencia de informes del consumidor y solicitarle que levante el congelamiento al menos tres días hábiles antes de presentar la solicitud. A partir del 1.º de septiembre de 2008, si se comunica con una agencia de informes del consumidor por un método electrónico seguro o por teléfono, la agencia de informes del consumidor debe levantar el congelamiento en el plazo de quince minutos. Usted tiene derecho a entablar una acción civil contra una agencia de informes del consumidor que viole sus derechos conforme a la Ley de Informes de Crédito Justos y Seguridad de la Identidad.
Nueva York	También puede obtener información sobre la respuesta a las violaciones de seguridad y la prevención y protección contra el robo de identidad en la Oficina del Fiscal General de Nueva York: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, www.ag.ny.gov.
Carolina del Norte	También puede obtener información sobre cómo prevenir y evitar el robo de identidad en la Oficina del Fiscal General de Carolina del Norte: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-919-716-6000, www.ncdoj.gov.
Oregón	Las leyes estatales le aconsejan denunciar cualquier sospecha de robo de identidad a las autoridades policiales, así como a la Comisión Federal de Comercio. La información de contacto del Departamento de Justicia de Oregón es la siguiente: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301, 1-877-877-9392, www.doj.state.or.us.
Rhode Island	Tiene derecho a presentar u obtener una denuncia policial relacionada con este incidente. También puede obtener información sobre cómo prevenir y evitar el robo de identidad en la Oficina del Fiscal General de Rhode Island: Office of the Attorney General, 150 South Main Street, Providence, RI, 02903, 1-401-274-4400, www.riag.ri.gov.