<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

DataHEALTH, Inc. ("DataHEALTH") is a cloud hosting and data storage company that provides services to certain health care providers, including <<b2b_text_1(Covered Entity Name)>>. We place a high value on maintaining the privacy and security of the information we maintain for our customers. Regrettably, we are writing to inform you that we recently learned of criminal conduct that resulted in a security incident that involved some of your personal information, which was stored by DataHEALTH in connection with the services we provide to <<b2b_text_1(Covered Entity Name)>>. This letter explains the incident, outlines the measures we have taken in response, and provides additional steps you can take to help protect your personal information.

What happened?

On November 3, 2021, DataHEALTH was the target of a criminal ransomware attack. Immediately upon learning of the incident, DataHEALTH undertook measures to contain the incident, launched an investigation, and engaged third-party cybersecurity forensic experts. On December 30, 2021, DataHEALTH learned that the unauthorized party obtained data from DataHEALTH's servers through a third-party software used by some DataHEALTH customers and that some of your personal information was compromised. At this time, DataHEALTH has no reason to believe this data was further used or disclosed by the unauthorized party. DataHEALTH conducted a thorough review of the data to identify individuals whose personal information may have been involved.

DataHEALTH has reported this information to the FBI and is actively cooperating with the FBI in its investigation.

What information was involved?

The review determined that the data involved contained some of your personal information, including your <<b2b_text_3(Name, Data Elements)>>.

What we are doing.

DataHEALTH has worked with the third-party software provider to update log-in credentials for all DataHEALTH customers that utilize the software. To help prevent a similar type of incident from occurring in the future, DataHEALTH implemented additional security protocols designed to enhance the security of DataHEALTH's network, internal systems and applications. DataHEALTH will also continue to evaluate additional steps that may be taken to further increase its defenses going forward. In addition, DataHEALTH is continuing to support federal law enforcement's investigation.

At this time, DataHEALTH has no indication that your personal information has been misused, but we wanted to make you aware of the incident and provide you with additional information on steps you may consider taking. To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until ***<<b2b_text_6(activation deadline)>>*** *to activate your identity monitoring services.*

Membership Number: **<<Membership Number s_n>>**

Additional information describing your services is included with this letter. For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via our automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through our automated phone system.

What you can do.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

If you have questions, please call (855) 618-3165, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time (excluding some U.S. holidays). Please have your membership number ready.

Again, the security of your personal information is important to DataHEALTH and <<b2b_text_1(Covered Entity Name)>>. We apologize for the stress and worry this situation has caused you and are doing everything we can to rectify the situation. Please remain vigilant reviewing account statements, credit reports, and explanation of benefits statements. Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

Ingrid Helgeson
Chief Operating Officer

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report 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 5 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, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

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

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

For residents of Rhode Island: You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, 401-274-4400, http://www.riag.ri.gov.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Triple Bureau Credit Monitoring and Single Bureau Credit Report

Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Aviso de filtración de datos

Estimado <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

DataHEALTH, Inc. ("DataHEALTH") es una empresa de almacenamiento de datos y alojamiento en la nube que brinda servicios a ciertos proveedores de atención médica, incluidos <<b2b_text_1(Covered Entity Name)>>. Damos un gran valor al mantenimiento de la privacidad y seguridad de la información que mantenemos para nuestros clientes. Lamentablemente, le escribimos para informarle que recientemente nos enteramos de una conducta delictiva que resultó en un incidente de seguridad que involucró parte de su información personal, que fue almacenada por DataHEALTH en relación con los servicios que brindamos a <<b2b_text_1(Covered Entity Name)>>. Esta carta explica el incidente, describe las medidas que hemos tomado en respuesta y brinda los pasos adicionales que puede tomar para ayudar a proteger su información personal.

¿Qué sucedió?

El 3 de noviembre de 2021, DataHEALTH fue el objetivo de un ataque de ransomware criminal. Inmediatamente después de enterarse del incidente, DataHEALTH tomó medidas para contener el incidente, inició una investigación y contrató a expertos forenses de ciberseguridad externos. El 30 de diciembre de 2021, DataHEALTH se enteró de que la parte no autorizada obtuvo datos de los servidores de Data HEALTH a través de un software de terceros utilizado por algunos clientes de DataHEALTH y que parte de su información personal estaba comprometida. En este momento, DataHEALTH no tiene motivos para creer que la parte no autorizada utilizó o divulgó estos datos. DataHEALTH realizó una revisión exhaustiva de los datos para identificar a las personas cuya información personal pudo haber estado involucrada.

DataHEALTH ha brindado esta información al FBI y está cooperando activamente con el FBI en su investigación.

¿Qué información se vio involucrada?

La revisión determinó que los datos involucrados contenían parte de su información personal, incluida su <<b2b_text_3(Name, Data Elements)>>.

Lo que estamos haciendo.

DataHEALTH ha trabajado con el proveedor de software externo para actualizar las credenciales de inicio de sesión de todos los clientes de DataHEALTH que utilizan el software. Para ayudar a evitar que ocurra un tipo de incidente similar en el futuro, DataHEALTH implementó protocolos de seguridad adicionales diseñados para mejorar la seguridad de la red, los sistemas internos y las aplicaciones de DataHEALTH. DataHEALTH también continuará evaluando los pasos adicionales que se pueden tomar para aumentar aún más sus defensas en el futuro. Además, DataHEALTH continúa apoyando la investigación de las fuerzas del orden público federales.

En este momento, DataHEALTH no tiene indicios de que su información personal haya sido mal utilizada, pero queremos informarle sobre el incidente y brindarle información adicional sobre los pasos que puede considerar tomar. A fin de ayudar a aliviar sus preocupaciones y recuperar la confianza después de este incidente, hemos contratado los servicios de Kroll para proporcionarle el servicio de monitoreo de identidad durante un año y sin costo alguno para usted. Kroll es un líder mundial en mitigación y respuesta ante riesgos y su equipo posee amplia experiencia en ayudar a personas que han sufrido una exposición involuntaria de datos confidenciales. Sus servicios de monitoreo de identidad incluyen monitoreo de crédito, un informe de crédito actual, Web Watcher, Public Persona, Quick Cash Scan, reembolso por pérdida de identidad por fraude de $ 1 millón, consulta de fraude y restauración de robo de identidad.

Visite **https://enroll.krollmonitoring.com** para activar y aprovechar los servicios de monitoreo de identidad.

Tiene hasta el ***<<b2b_text_6(activation deadline)>>*** *para activar sus servicios de monitoreo de identidad.*

Número de membresía: **<<Membership Number s_n>>**

En esta carta, se incluye información adicional que describe sus servicios. Si desea obtener más información sobre Kroll y sus servicios de monitoreo de identidad, visite info.krollmonitoring.com.

Si prefiere activar estos servicios sin conexión a Internet y recibir alertas de monitoreo a través del Servicio Postal de EE. UU., puede activarlos mediante nuestro sistema telefónico automatizado llamando al 1-888-653-0511, de lunes a viernes, de 8:00 a. m. a 5:30 p. m. Hora Central, excepto los principales días festivos de EE. UU. Tenga a la mano su número de membresía, que se encuentra en su carta, cuando llame. Tenga en cuenta que, para activar los servicios de monitoreo, deberá proporcionar su nombre, fecha de nacimiento y número de seguro social a través del sistema telefónico automatizado.

Lo que puede hacer.

Revise la sección “Recursos adicionales” adjunta que se incluye con esta carta. Esta sección describe los pasos adicionales que puede tomar para ayudar a protegerse, incluidas las recomendaciones de la Comisión Federal de Comercio con respecto a la protección contra el robo de identidad y detalles sobre cómo colocar una alerta de fraude o un congelamiento de seguridad en su archivo de crédito.

Para obtener más información.

Si tiene alguna pregunta, llame al (855) 618-3165, de lunes a viernes, de 8:00 a. m. a 5:30 p. m. Hora central (excepto algunos días festivos de EE. UU.) Tenga a la mano su número de membresía.

Una vez más, la seguridad de la información personal de su hijo es importante para DataHEALTH y <<b2b_text_1(Covered Entity Name)>>. Nos disculpamos por el estrés y la preocupación que esta situación le ha causado y estamos haciendo todo lo posible para corregir la situación. Permanezca alerta al revisar los estados de cuenta, los informes de crédito y la explicación de las declaraciones de beneficios. La protección de su información es importante para nosotros. Confiamos en que los servicios que le ofrecemos demuestren nuestro compromiso continuo con su seguridad y satisfacción.

Atentamente,

Ingrid Helgeson
Directora de operaciones

RECURSOS ADICIONALES

La información de contacto de las tres agencias de informes de crédito a nivel nacional es:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Informe de crédito gratuito. Se recomienda que permanezca atento que revise los estados de cuenta y controle su informe de crédito para detectar actividades no autorizadas, especialmente actividades que puedan indicar fraude y robo de identidad. Puede obtener una copia de su informe de crédito, de forma gratuita, una vez cada 12 meses de cada una de las tres agencias de informes de crédito a nivel nacional.

Para solicitar su informe anual de crédito gratuito, visite **www.annualcreditreport.com** o llame sin cargo al **1-877-322-8228**.

También puede solicitar su informe anual de crédito gratuito enviando por correo un Formulario de solicitud de informe anual de crédito completo (disponible en el sitio web de la Comisión Federal de Comercio de EE. UU. ("FTC") en www.consumer.ftc.gov) a:

Servicio de solicitud de informe anual de crédito, PO Box 105281, Atlanta, GA 30348-5281.

Para los residentes de Colorado, Georgia, Maine, Maryland, Massachusetts, Nueva Jersey, Puerto Rico y Vermont: pueden obtener una o más copias adicionales (según el estado) de su informe de crédito, de manera gratuita. Debe comunicarse con cada una de las agencias de informes de crédito directamente para obtener dichos informes adicionales.

Alertas de fraude. Hay dos tipos de alertas de fraude que puede colocar en su informe de crédito para informar a sus acreedores de que puede ser víctima de fraude: una alerta inicial y una alerta extendida. Puede solicitar que se coloque una alerta inicial de fraude en su informe de crédito si sospecha que ha sido o víctima de robo de identidad o que está a punto de serlo. Una alerta inicial de fraude permanece en su informe de crédito durante al menos un año. Puede solicitar que se coloque una alerta extendida en su informe crediticio si ya ha sido víctima de un robo de identidad y presenta la prueba documental adecuada. Una alerta extendida de fraude permanece en su informe de crédito durante siete años. Puede colocar una alerta de fraude en su informe de crédito comunicándose con cualquiera de las tres agencias nacionales de informes de crédito.

Congelamiento de seguridad. Tiene la opción de aplicar un bloqueo de seguridad, conocido también como congelamiento de crédito, en su informe de crédito, sin costo.

El congelamiento de seguridad tiene por finalidad evitar que se aprueben créditos, préstamos y servicios en su nombre sin su consentimiento. Para aplicar un congelamiento de seguridad en su informe de crédito, podrá hacerlo a través de proceso en línea, una línea telefónica automatizada o una solicitud por escrito a cualquiera de las tres agencias nacionales de informes de crédito mencionadas anteriormente. Al solicitar un congelamiento de seguridad debe incluir la siguiente información (tenga en cuenta que, si está solicitando un informe de crédito para su cónyuge debe incluir esta información para él/ella también): (1) nombre completo, con inicial del segundo nombre y cualquier sufijo de tratamiento; (2) número de Seguro social; (3) fecha de nacimiento; (4) dirección actual y todas las direcciones que pueda haber tenido en los últimos 5 años; y (5) cualquier informe de incidentes o denuncias que haya presentado a la policía o al Registro de vehículos automotores. La solicitud también debe incluir una copia de un documento de identificación emitido por el gobierno y unacopia reciente de un recibo de luz o agua o un estado de cuenta bancario o del seguro. Es indispensable que cada copia sea legible, esté a su nombre y que indique su dirección postal actual y la fecha de emisión.

Comisión Federal de Comercio y Fiscalías Generales del Estado. Si cree que es víctima de robo de identidad o tiene motivos para creer que su información personal ha sido utilizada indebidamente, debe comunicarse de inmediato con la Comisión Federal de Comercio o con la Fiscalía General de su estado de origen. También puede comunicarse con estas agencias para solicitar información sobre cómo impedir o minimizar el riesgo del robo de identidad.

Puede contactar a la **Comisión Federal de Comercio**, Centro de Respuesta al Consumidor, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

Para residentes de Maryland: pueden comunicarse con la Fiscalía General de Maryland, División de Protección al Consumidor, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

Para los residentes de Carolina del Norte: pueden comunicarse con la Fiscalía General de Carolina del Norte, División de Protección al Consumidor, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

Para los residentes de Nueva York: pueden contactarse con el Fiscal General a través de la Fiscalía General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

Para los residentes de Connecticut: pueden comunicarse con la Oficina del Fiscal General de Connecticut, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

Para los residentes de Massachusetts: pueden comunicarse con la oficina del Fiscal General de Massachusetts, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Para residentes de Rhode Island: también pueden obtener información sobre cómo prevenir y evitar el robo de identidad en la Oficina del Fiscal General de Rhode Island: Oficina del Fiscal General de Rhode Island, Unidad de Protección al Consumidor, 150 South Main Street, Providence, RI 02903, 401-274-4400, http://www.riag.ri.gov.

Denuncia de robo de identidad y obtención de una denuncia policial.

Para los residentes de Iowa: se les aconseja informar de cualquier sospecha de robo de identidad a la policía o al Fiscal General de Iowa.

Para los residentes de Massachusetts: tienen derecho a obtener una denuncia policial si es víctima de robo de identidad.

Para los residentes de Oregon: Se les aconseja informar de cualquier sospecha de robo de identidad a la policía, a la Comisión Federal de Comercio y al Fiscal General de Oregon.

Para los residentes de Rhode Island: Según la ley de Rhode Island, usted tiene derecho a obtener cualquier informe policial presentado con respecto a este incidente.

KROLL

APROVECHE SUS SERVICIOS DE MONITOREO DE IDENTIDAD

Se le ha brindado acceso a los siguientes servicios de Kroll:

Supervisión de crédito de triple oficina e informe de crédito de oficina única

Su informe de crédito actual está disponible para que lo revise. Usted recibirá alertas cuando haya cambios en sus datos crediticios en cualquiera de las tres agencias de informes crediticios nacionales, por ejemplo, cuando una nueva línea de crédito se solicita en su nombre. Si no reconoce la actividad, tendrá la opción de llamar a un especialista en fraude de Kroll, que podrá ayudarlo a determinar si se trata de un indicador de robo de identidad.

Web Watcher

Web Watcher supervisa los sitios de Internet donde los delincuentes pueden comprar, vender e intercambiar información de identidad personal. Se generará una alerta si se encuentra evidencia de su información de identidad personal.

Public Persona

Public Persona monitorea y notifica cuando los nombres, alias y direcciones se asocian con su número de Seguro Social. Si se encuentra información, recibirá una alerta.

Quick Cash Scan

Quick Cash Scan monitorea las fuentes de préstamos a corto plazo y de anticipo de efectivo. Recibirá una alerta cuando se informe un préstamo y puede llamar a un especialista en fraudes de Kroll para obtener más información.

Reembolso de pérdida por fraude de identidad de $1 millón

Le reembolsa los gastos de bolsillo por un total de hasta $1 millón en costos y gastos legales cubiertos por cualquier evento de robo de identidad. Toda cobertura está sujeta a las condiciones y exclusiones de la póliza.

Asesoría sobre fraude

Tiene acceso ilimitado para realizar consultas con un especialista en fraude de Kroll. El asesoramiento incluye mostrarle las formas más efectivas de proteger su identidad, explicarle sus derechos y protecciones en virtud de la ley, ofrecer asistencia con las alertas de fraude e interpretar cómo se accede y utiliza la información personal, incluyendo la investigación de actividades sospechosas que podrían estar vinculadas con un incidente de robo de identidad.

Restauración por robo de identidad

Si resulta ser víctima de un robo de identidad, un investigador experto autorizado de Kroll trabajará en su representación para resolver cualquier problema relacionado. Tendrá acceso a un investigador especializado que entiende sus problemas y que puede realizar la mayor parte del trabajo por usted. El investigador podrá investigar a fondo para revelar todos los aspectos del robo de identidad y, luego, trabajar para resolverlo.

El sitio web de activación de Kroll solo es compatible con la versión actual o una versión anterior de Chrome, Firefox, Safari y Edge.

Para recibir servicios de crédito, usted debe ser mayor de 18 años y tener un crédito en EE. UU., tener un número de seguro social a su nombre, así como un domicilio de residencia en EE. UU. asociado a su expediente de crédito.