Aviso de incidente de seguridad / Notificación de violación de datos

El bufete de abogados Carlson Law Firm ("Carlson" o "nosotros") está notificando a las personas potencialmente afectadas sobre un reciente evento de ciberseguridad. No hay pruebas de que se haya utilizado indebidamente su información personal. La seguridad de la información personal de nuestros clientes es muy importante para nosotros y pedimos sinceras disculpas por cualquier inconveniente que esto pueda causar.

¿Qué ocurrió?

Carlson identifico actividades sospechosas asociadas con nuestros sistemas informáticos. En cuanto nos enteramos de la actividad, tomamos medidas inmediatas para proteger nuestro entorno y contratamos expertos forenses informáticos independientes para ayudar en la investigación. La investigación concluyó que un actor no autorizado accedió a nuestra red y pudo haber tomado documentos almacenados en la red durante el incidente. Estos documentos no forman parte de nuestros archivos actuales de casos ni de almacenamiento activo de datos y se mantuvieron por separado de los sistemas que utilizamos actualmente para mantener asuntos y registros de clientes. La información almacenada en el servidor era compleja y no fácilmente consultable, pero podía incluir información personal relacionada con ciertos clientes representados.

El tipo de información afectada incluye nombres y alguna combinación de lo siguiente: direcciones, fechas de nacimiento, números de Seguro Social, números de licencia de conducir u otras identificaciones emitidas por el gobierno, tratamiento y diagnóstico de salud, y facturas de tratamiento médico.

De nuevo, no tenemos pruebas de ningún uso indebido de la información, pero estamos notificando por precaución. Hemos mejorado nuestro programa de seguridad de la información implementando controles adicionales, como el despliegue de software de detección de puntos finales en todos nuestros sistemas, el cambio de todas las contraseñas de usuario y sistema, y el endurecimiento de los controles de acceso.

Lo que puede hacer:

Le recomendamos mantenerse atento a posibles señales de robo de identidad mediante la revisión periódica de sus estados de cuenta bancarios y otros registros financieros. Si detecta alguna actividad sospechosa, comuníquese de inmediato con su institución financiera. También puede consultar la página de la Comisión Federal de Comercio (Federal Trade Commission) para obtener más información sobre cómo proteger su identidad en línea a https://consumidor.ftc.gov/robo-de-identidad-y-seguridad-en-linea.

Para más información:

Para más información sobre los pasos que puede tomare para proteger su información, consulte las recomendaciones que se ofrecen a continuación. Aunque no tenemos motivos para creer que se haya utilizado indebidamente ninguna información personal , queremos disculparnos por cualquier inconveniencia que esto pueda causarle.

Si tiene más preguntas o inquietudes, por favor contáctenos en notification@carlsonattorneys.com o llama al 855-292-1148. Los correos electrónicos serán respondidos en un plazo de dos días laborables y las llamadas se responderán entre las 8:00 y las 17:00, hora central, de lunes a viernes.

Pasos recomendados para ayudar a proteger tu información:

1. Revise sus informes de crédito. Le recomendamos vigilar sus estados de cuenta y revisar periódicamente sus informes de crédito. Además, la ley federal le permite obtener una copia gratuita de su informe de crédito cada 12 meses de cada una de las tres principales agencias de informes de crédito. Para obtener un informe de crédito anual gratuito, accede a www.annualcreditreport.com o llama al 1-877-322-8228. Podría escalonar sus solicitudes para recibir un informe gratuito de una de las tres agencias de crédito cada cuatro meses.

Además, usted tiene derecho a presentar una denuncia policial si llega a ser víctima de robo de identidad. Para reporta este delito ante las autoridades es posible que deba aportar documentación que demuestre que fue afectado. Con frecuencia, se exige un informe policial pare impugnar cargos o registros fraudulentos. También puede reportar actividad sospechosa de robo de identidad a las autoridades locales o al Fiscal General.

2. Colocar alertas de fraude en las tres agencias de crédito. Si decide colocar una alerta de fraude, te recomendamos hacerlo después de activar su monitorización de crédito. Puede enviar una alerta de fraude a una de las tres principales agencias de crédito por teléfono y también a través de la web de Experian o Equifax. Una alerta de fraude indica a los acreedores que sigan ciertos procedimientos, incluyendo comunicarse con usted, antes de abrir nuevas cuentas o cambiar sus cuentas existentes. Por eso, poner una alerta de fraude puede protegerlo, pero también puede retrasarlo cuando busque obtener crédito. La información de contacto de las tres oficinas es la siguiente:

Agencias de crédito

Denuncia de fraude en Equifax 1-866-349-5191 P.O. Box 105069 Atlanta, GA 30348-5069 www.equifax.com	Informe de fraude de Experian 1-888-397-3742 P.O. Box 9554 Allen, TX 75013 www.experian.com	Denuncia de fraude de TransUnion 1-800-680-7289 P.O. Box 2000 Chester, PA 19022-2000 www.transunion.com

Es necesario contactar solo UNA de estas agencias y utilizar solo UNO de estos métodos. En cuanto una de las tres agencias confirme su alerta de fraude, las demás son notificadas para que también incluyan alertas en sus registros.

Recibirá cartas de confirmación por correo y podrá solicitar los tres informes de crédito, sin costo alguno, para su revisión, Una alerta inicial de fraude durara un año.
Por favor, tenga en cuenta: Nadie puede colocar una alerta de fraude en tu informe de crédito excepto tú.

3. Congelación de seguridad / crédito. Un congelamiento de seguridad / crédito puede ayudar a impedir que otra persona use su información personal para abrir nuevas cuentas o solicitar crédito a su nombre. Para activarlo, debe comunicarse con las tres agencias nacionales de informes de crédito mencionadas anteriormente. Tenga en cuenta que, mientras el congelamiento esté vigente, nadie podrá obtener nuevos préstamos, crédito instantáneo o tarjetas de crédito hasta que lo suspenda temporalmente o lo elimine. Congelar y descongelar su archivo de crédito no tiene costo.

4. Puede obtener información adicional sobre cómo prevenir el robo de identidad a través de la Comisión Federal de Comercio (FTC). Si considera que su información ha sido utilizada indebidamente, el FTC le urge presentar una queja ante esa agencia.

Residentes de EE. UU.: Centro de Atención sobre Robo de Identidad, Comisión Federal de Comercio, 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.consumer.gov/idtheft; 1-877-IDTHEFT (438-4338); TTY: 1-866-653-4261.