Notificación de Violación de Datos
8 de julio de 2019

En cumplimiento con las leyes federales y estatales, esto proporciona un aviso alternativo.

Nemadji brinda servicios de detección de elegibilidad y facturación de pacientes para el Departamento de Servicios de Salud (DHS por sus siglas en inglés) del Condado de Los Ángeles. Como socio comercial del Departamento de Servicios de Salud, respetamos la privacidad de su información y tomamos muy en serio la privacidad del paciente. Este aviso es para informarle de una violación de datos que puede involucrar la información personal de 14.591 pacientes del Departamento de Servicios de Salud, y es importante para nosotros que usted esté completamente informado de este asunto reciente.

¿Qué Sucedió?
El 28 de marzo de 2019, un empleado de Nemadji fue víctima de un ataque de phishing por correo electrónico. Un correo electrónico de phishing intenta engañar a alguien para que dé información importante al hacerse pasar como proveniente de una fuente confiable. Las cuentas de correo electrónico son utilizadas por empleados de Nemadji para comunicarse y realizar servicios para DHS. El correo electrónico de phishing comprometió una cuenta de correo electrónico y dio lugar a la violación de datos actual. El 26 de junio de 2019, Nemadji le confirmó a DHS que el ataque de phishing puede haber afectado a los pacientes de DHS, pero no hay evidencia que sugiere que información personal relacionada con los pacientes de DHS fue específicamente dirigido por el evento de phishing.

¿Qué información estuvo involucrada?
La información personal de los pacientes de DHS presentes en la cuenta de correo electrónico en el momento del incidente varió según el individuo, pero pudo haber incluido el nombre y apellido y uno o más de los siguientes elementos de datos: dirección, fecha de nacimiento, número de teléfono, mes y año de servicio. También se identificó el número de seguro social de dos pacientes y códigos de diagnóstico de cuatro pacientes. No se expuso ninguna información médica específica.

¿Qué está haciendo Nemadji?
Nemadji valora la privacidad del paciente y lamenta profundamente que haya ocurrido este incidente. Al descubrir la infracción, hemos tomado medidas inmediatas para evitar otro mayor acceso y comenzamos a trabajar estrechamente con los proveedores de seguridad cibernética para asegurarnos de que el incidente se resuelva de manera adecuada. Nemadji ha iniciado una revisión administrativa, se examinaron y revisaron los procesos para mejorar la seguridad y se implementaron controles adicionales diseñados para prevenir la repetición de dicho incidente. Además, Nemadji también ha mejorado la capacitación de la fuerza laboral para identificar y responder ante los correos electrónicos de phishing.

Además de notificar a las personas potencialmente afectadas por este incidente, se le informó a la Oficina Federal de Investigación. También notificaremos a la Fiscalía General del Estado y a la Oficina de Derechos Civiles del Departamento de Salud y Servicios Humanos de los Estados Unidos, tal como lo exige la ley.

¿Qué pude hacer usted?
Aunque Nemadji no tiene conocimiento de ningún uso actual o intento de uso indebido de información como resultado de este incidente, para ayudar a aliviar las inquietudes y recuperar la confianza después de este incidente, hemos asegurado los servicios de Kroll para proporcionar monitoreo de identidad a las personas potencialmente afectadas, sin

costo alguno por un año. Kroll es un líder mundial en mitigación y respuesta de riesgos, y su equipo tiene una amplia experiencia ayudando a personas que han sufrido una exposición involuntaria de datos confidenciales.

Para recibir servicios de crédito por correo en lugar de en línea (por internet) las personas afectadas pueden llamar al 1-800-491-4740. A continuación, se muestra información adicional que describe los servicios.

Por favor revise a continuación la sección de "Recursos Adicionales". Esta sección describe los pasos adicionales que puede tomar para ayudar a protegerse, incluyendo las recomendaciones por parte de la Comisión Federal de Comercio con respecto a la protección de robo de identidad y detalles sobre cómo colocar una alerta de fraude y congelamiento de seguridad en su archivo de crédito.

Para más información

Si tiene preguntas, por favor llame al 1-800-491-4740, de lunes a viernes de 8:00 a.m. a 5:30 p.m. hora del pacífico.

Para nosotros es importante proteger su información. Confiamos en que los servicios que le ofrecemos demuestren nuestro compromiso continuo con su seguridad y satisfacción.

RECURSOS ADICIONALES

Control de cuentas

Le alentamos a que esté atento a incidentes de robo de identidad y fraude, que revise sus resúmenes de cuentas bancarias, resúmenes de tarjetas de crédito o débito, informes de pólizas de seguros médicos, informes crediticios y formularios de explicación de beneficios para detectar actividades sospechosas. Conforme a la ley de los Estados Unidos, usted tiene derecho a solicitar un informe crediticio anual gratis de cada una de las tres principales agencias de informes de crédito. Para solicitar su informe crediticio gratuito, visite www.annualcreditreport.com o llame sin cargo al 1-877-322-8228. También puede ponerse en contacto directamente con las tres principales agencias de informes de crédito para solicitar una copia gratuita de su informe crediticio.

Tiene el derecho de colocar un "congelamiento de seguridad" sobre su informe crediticio, que evitará que una agencia de informes de solvencia divulgue información en su informe crediticio si no lo autoriza de forma explícita. El congelamiento de seguridad está diseñado para evitar que se aprueben créditos, préstamos y servicios en su nombre sin su consentimiento. Sin embargo, debe saber que usar un congelamiento de seguridad para poder controlar quién obtiene acceso a la información personal y financiera de su informe crediticio puede demorar, interferir o impedir la autorización oportuna de cualquier solicitud o petición que usted haga a posteriori con respecto a un préstamo, crédito o hipoteca nueva o a cualquier otra cuenta que implique la concesión de un crédito. Conforme a la ley federal, no le pueden cobrar por colocar o quitar un congelamiento de seguridad de su informe crediticio. Si desea colocar un congelamiento de seguridad, póngase en contacto con las principales agencias de informes de solvencia que se mencionan a continuación:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

Para poder solicitar un congelamiento de seguridad, deberá proporcionar la siguiente información:

1. Nombre completo (incluida la inicial del segundo nombre, así como los sufijos Jr., Sr., II, III, etc.)
2. Número de Seguro Social
3. Fecha de nacimiento
4. Si se mudó en los últimos cinco (5) años, indique los domicilios en los que vivió en el transcurso de este tiempo.
5. Comprobante del domicilio actual, como una factura actual de un servicio o una factura telefónica
6. Una fotocopia legible de un documento de identidad emitido por un organismo gubernamental (licencia de conducir estatal o documento de identidad, identificación militar, etc.).
7. Si usted es víctima de un robo de identidad, incluya una copia de la denuncia policial, del informe de investigación de la denuncia efectuada ante un organismo de seguridad encargado de tratar con el delito de robo de identidad.

Como alternativa a un congelamiento de seguridad, tiene el derecho a incluir sin cargo en su historial una "alerta de fraude" preliminar o prolongada. Una alerta de fraude preliminar es una alerta de 1 año, que se incluye en el historial de crédito del consumidor. Si una empresa ve una alerta de fraude en el historial de crédito de un consumidor, debe tomar medidas para verificar la identidad del consumidor antes de conceder un crédito nuevo. Si usted fue víctima de un robo de identidad, tiene derecho a implementar una alerta de fraude prolongada, que es una alerta que dura siete años. Si desea colocar una alerta de fraude, póngase en contacto con cualquiera de las agencias que se mencionan a continuación:

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com/fraud-victim-resources/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Información adicional

Además, puede instruirse sobre el robo de identidad, las alertas de fraude, los congelamientos de seguridad y los pasos que puede seguir para protegerse. Para ello, póngase en contacto con las agencias de informes de solvencia, con la Comisión Federal de Comercio o con el fiscal general del Estado.

Puede acercarse a la Comisión Federal de Comercio de las siguientes maneras: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. La Comisión Federal de Comercio también sugiere que toda aquella persona que haya descubierto que su información ha sido utilizada indebidamente presente una denuncia ante ellos. Puede obtener más información sobre cómo presentar una demanda por medio de la información de contacto que se indica a continuación. Tiene derecho a hacer una denuncia policial si fue víctima de un robo de identidad o fraude. Tenga en cuenta que, para poder hacer una denuncia ante una autoridad policial por robo de identidad, probablemente necesite presentar alguna prueba de que fue víctima de ese delito. También se debe denunciar ante agentes policiales ocasiones de robo de identidad presuntas o reales. Este aviso no fue retrasado por las autoridades policiales.