COUNTY OF KERN
MENTAL HEALTH DEPARTMENT
Bill Walker, LMFT, Director

Working together toward
Hope, Recovery and Independence

Estimados residentes del Condado de Kern,

Esta carta es para informarles de un incidente de seguridad que ocurrió recientemente el 15/04/16 en las oficinas de la administración de Salud Mental del Condado de Kern.

Nuestras oficinas de administración fueron reubicadas recientemente. Durante la mudanza, sin intención, un reporte se quedó en una parte desocupada del edificio que había estado bajo construcción. Tenga en cuenta que la información contenida en el informe se limita a nombre y apellido, nuestro propio número interno de expediente clínico, un código de servicio interno y la unidad asociada donde se proporcionaron los servicios. Este informe no contiene información sobre el tratamiento del individuó o cualquier otra información como números de seguro social, números de licencia de conducir, o números de cuentas financieras que podrían exponerlos al robo de identidad. No obstante, creemos que es necesario informarles de que varios contratistas habían estado trabajando en el edificio y habrían tenido acceso al informe.

Los servicios identificados en el informe (por número de código solamente) fueron proporcionados por el Departamento de Salud Mental del Condado de Kern así como varios proveedores bajo contrato con el Departamento de Salud Mental y el Departamento de Uso de Sustancias durante el periodo de 01/09/06 a 30/09/06. Todas las páginas de este informe han sido contabilizadas, están en el orden correcto, y no hay indicación obvia que alguien haya visto el informe. Sin embargo, debido a que fue descubierto en un área desatendida por el personal, queremos informarle de este incidente de seguridad. Una vez más, los únicos beneficiarios afectados fueron los que recibieron servicios durante este período de un mes (septiembre del 2006).

Lamentamos que se produjo este incidente y les aseguramos que estamos analizando y revisando nuestros procedimientos y prácticas para reducir el riesgo de recurrencia.

Favor de guardar una copia de este aviso en su registro personal en caso de problemas con su historial médico en el futuro. Si desea, también puede solicitar una copia de su historial clínico del Departamento de Salud Mental del Condado de Kern, para servirle como base. Para información sobre sus derechos de privacidad médica, puede visitar la página web del Departamento de Justicia, Privacidad y Protección de Aplicación de California: **www.privacy.ca.gov**. Para obtener nuestra póliza completa de privacidad o enlaces de web a información para aquellos que puedan verse afectados, visite nuestra página web: **www.co.kern.ca.us/kcmh**.

En caso que necesite más información sobre este incidente, por favor llame a la línea directa y gratuita de **PRIVACIDAD Y CONFORMIDAD** al (888) 875-5559.

3300 Truxtun Ave. • P.O. Box 1000 • Bakersfield, CA 93302
Voice: (661) 868-6600 • FAX: (661) 868-6666 • TTY Relay: 1-800-735-2929

Ayuda en caso de robo de datos confidenciales

Consejos para el consumidor del Procurador General de California

Hoja 17 de información al consumidor • Octubre de 2014

Suponga que recibe una carta de una compañía, agencia del gobierno, una universidad, un hospital u otra organización, La carta dice que su información personal puede haber formado parte de un robo de datos confidenciales. O quizás se entere del episodio por un boletín de noticias o sitio web de la empresa. Cualquiera sea la manera en que reciba la información, el hecho de que se haya violado la seguridad de los datos de una compañía no quiere decir que usted haya caído víctima de robo de identidad o sufrido un daño, pero existe el riesgo de que así sea.

El aviso de violación de datos confidenciales debería indicar los tipos específicos de información personal involucrados. También le puede decir lo que la organización está haciendo para contrarrestar el problema. Para protegerse a sí mismo, puede tomar los pasos que se indican a continuación. Todo dependerá del tipo de información personal afectada en el robo de los datos confidenciales.

Algunas compañías afectadas le ofrecerán sin cargo una alerta de crédito, lo cual le alerta después de que alguien solicitó u obtuvo un crédito nuevo en su nombre. La alerta de crédito puede ser útil cuando le roban su número del Seguro Social. Pero no le avisa cuando se produce actividad fraudulenta en su cuenta existente de tarjeta de crédito o débito.

Número de tarjeta de crédito o débito

El aviso de robo de datos confidenciales quizás le informe cuándo y dónde se produjo dicha violación. Si usó su tarjeta de crédito o débito en ese lugar en el periodo indicado, puede tomar pasos para protegerse.

Tarjeta de crédito

1. Vigile su cuenta de tarjeta de crédito para ver si hay transacciones sospechosas, y denúncielas al banco que emitió la misma (o a American Express o Discover). Pídale al banco que habilite la vigilancia y alertas en línea para esa cuenta. De esa manera podrá recibir un aviso anticipado de cualquier transacción fraudulenta.

2. Si observa transacciones fraudulentas en su tarjeta de crédito después de haberse anunciado el robo de datos confidenciales, considere la posibilidad de cancelar su tarjeta de crédito. Puede disputar las transacciones fraudulentas que aparezcan en su estado de cuenta, y deducirlas del monto adeudado. Su responsabilidad por transacciones fraudulentas se limita a $50 cuando las denuncia, y la mayoría de los bancos tienen políticas que lo eximen a usted de toda responsabilidad.[1]

Kamala D. Harris
Attorney General
State of California

California Department of Justice
Privacy Enforcement and Protection Unit
www.oag.ca.gov/privacy

3. Si cancela su tarjeta de crédito, no se olvide de comunicarse con todas las compañías que deducen sus pagos de la tarjeta en forma automática. Si quiere seguir haciendo pagos en forma automática, deles su nuevo número de cuenta.

Tarjeta de débito

1. Vigile su cuenta de tarjeta de débito para ver si hay transacciones sospechosas, y denúncielas a su banco. Pídale al banco que habilite la vigilancia y alertas en línea para esa cuenta. De esa manera podrá recibir un aviso anticipado de cualquier transacción fraudulenta.

2. Denuncie toda transacción no autorizada a su banco inmediatamente para evitar responsabilidad. Su responsabilidad por transacciones fraudulentas se limita a $50 si las reporta en un plazo de dos días. Su banco puede tener llegar a eximirlo de toda responsabilidad. Pero si deja pasar el tiempo, su responsabilidad aumentará, hasta llegar al monto total de la transacción si no la reporta en un plazo de 60 días de su aparición en su estado de cuenta.[2]

3. Considere la posibilidad de cancelar su tarjeta de débito. Esta tarjeta está conectada con su cuenta bancaria. La manera más segura de protegerse contra la posibilidad de que le saquen dinero de su cuenta bancaria con un número robado es cancelar la tarjeta. Si bien es probable que le devuelvan el dinero robado, es posible que esto no ocurra hasta que su banco haya completado su investigación.

Número del Seguro Social

Si el aviso le dice que quizás le han robado su número del Seguro Social, tiene que hacer lo siguiente.

1. Comuníquese con las tres agencias de información de crédito. Puede denunciar un robo potencial de identidad a las tres agencias principales de información de crédito llamando a cualquiera de los números gratis para denunciar fraude que aparecen a continuación. Lo atenderá un sistema telefónico automatizado que le permitirá marcar su expediente con un alerta de fraude en las tres agencias de información de crédito. También le enviarán instrucciones sobre cómo obtener una copia de su informe de cada una de las agencias de información de crédito.

Experian	1-888-397-3742
Equifax	1-800-525-6285
TransUnion	1-800-680-7289

2. Qué significa poner una alerta de fraude en su expediente de crédito. Una alerta de fraude ayuda a protegerlo contra la posibilidad de que un ladrón de identidad abra una cuenta de crédito en su nombre. Cuando un comerciante verifica el historial de crédito de alguien que está solicitando una cuenta de crédito, recibirá un aviso de que puede haber fraude en la cuenta. Esto alertará al comerciante para que tome los pasos necesarios para verificar la identidad del solicitante. Un alerta de fraude dura 90 días y se puede renovar. Para obtener información sobre un nivel de protección aún mayor, lea ***How to Freeze Your Credit Files*** *(Cómo congelar sus datos de crédito)* en *www.oag.ca.gov/privacy/info-sheets.*

3. Revise sus informes de crédito. Examine cada uno de ellos cuidadosamente. Fíjese si hay alguna cuenta que no reconoce, sobre todo cuentas abiertas recientemente. Fíjese en la sección de consultas *(inquiries)* para ver si hay nombres de acreedores a quienes usted no les solicitó crédito. Algunas compañías facturan con nombres distintos

que el de su tienda. La agencia de información de crédito le podrá decir cuando éste sea el caso. Algunas consultas pueden ser identificadas como "promocionales". Estas son cuando una empresa le ha pedido a una agencia de información de crédito su nombre y dirección para enviarle una oferta de crédito. Las consultas promocionales no son señales de fraude. (Cuando coloque una alerta de fraude, lo borrarán automáticamente de las listas para recibir ofertas de este tipo que usted no solicitó.) Además, como precaución general, fíjese en la sección sobre información personal para ver si hay alguna dirección donde usted nunca vivió.

4. Si encuentra algo que no comprende en su informe de crédito, llame a la agencia, al número que aparece en el informe. El personal de la agencia de información de crédito repasará el informe con usted. Si la información no se puede explicar, tendrá que llamar a los acreedores correspondientes y denunciar el delito en su comisaría local u oficina del alguacil.

Nombre de usuario y contraseña

En el caso de que la violación de seguridad de los datos involucre la contraseña de su cuenta en línea, quizás reciba un mensaje por correo electrónico o cuando inicie una sesión en la página web de su cuenta. Si se entera que quizás le han robado su nombre de usuario y contraseña, o su dirección de correo electrónico o la respuesta a sus preguntas de seguridad, puede tomar los siguientes pasos.

1. Cambie la contraseña de la cuenta afectada. Si no puede ingresar en su cuenta, comuníquese con el servicio al cliente o departamento de seguridad de la compañía.

2. Si usa la misma contraseña en otras cuentas, cámbielas también.

3. Si le robaron su respuesta a la pregunta de seguridad, cámbiela. No use preguntas de seguridad cuya respuesta se puede obtener por un medio público, como el nombre de soltera de su madre, el nombre de su mascota o el nombre de su escuela.

4. Use contraseñas distintas para cada una de sus cuentas en línea. Esto es particularmente importante para cuentas que tienen información sensible, como sus datos médicos o financieros. Tenga en cuenta, por ejemplo, que algunas de sus cuentas en línea pueden tener almacenado el número de su tarjeta de crédito.

5. Genere contraseñas robustas. Cuanto más largas, mejor. Deberían tener por lo menos diez caracteres, con una mezcla de mayúsculas, minúsculas, números, signos de puntuación y símbolos. No use palabras que se pueden encontrar en el diccionario. Puede basar sus contraseñas en una frase, canción o título de un libro.

   Ejemplo: "Viaje al centro de la Tierra" se puede convertir en V1aj3. al.c3ntr0.d3.la.Ti3rra

6. Un programa de administración de contraseñas o "caja fuerte" de contraseñas puede ayudarle a crear y administrar muchas contraseñas robustas. Estos programas pueden funcionar en su computadora, teléfono u otros dispositivos portátiles. Solo tiene que recordar una contraseña (o frase) para abrir la caja fuerte. La organización Electronic Frontier Foundation *(www.eff.org)* lista algunas versiones gratis, y puede ver análisis de estos productos en las revistas de informática.

Información bancaria

Si el aviso sobre la violación de seguridad datos le informa que quizás le robaron su número de cuenta bancaria, por ejemplo de una copia de su cheque, tome los siguientes pasos.

1. Llame al banco e infórmeles sobre la violación. Dígales que quiere cerrar su cuenta. Averigüe si hay cheques suyos que todavía no se cobraron. Quizás le convenga esperar hasta que se hayan cobrado antes de cerrar la cuenta. (O puede escribirle a cada uno de sus acreedores, informarles sobre la violación de datos, incluir un cheque de su cuenta nueva y pedirles que no cobren el cheque que les envió anteriormente.)

2. Abra una nueva cuenta bancaria. Dígale al banco que quiere usar una nueva contraseña para acceder a su nueva cuenta. No use el nombre de soltera de su madre o las últimas cuatro cifras de su número del Seguro Social. Pídale a su banco que notifique a su compañía de verificación de cheques que la cuenta anterior se ha cerrado.

Número de licencia de manejar

Si el aviso de violación de la seguridad de datos le informa que quizás le hayan robado su número de licencia para manejar o tarjeta de identificación de California, y sospecha que puede haber sido víctima de un robo de identidad, comuníquese con la Unidad de Análisis y Fraude de Licencias de Manejar (DL-FAU, por sus siglas en inglés) del DMV llamando al 1 866-658-5758 o escribiendo a *dlfraud@dmv.ca.gov*. No incluya ninguna información personal si escribe por correo electrónico.

Información de su seguro médico o de salud

Si el aviso le indica que quizás le robaron su número de seguro de salud o plan de salud, tome los siguientes pasos para protegerse contra un posible robo de identidad médica. Una violación de su información médica que no incluya su número del seguro o plan de salud en general no presenta un riesgo de robo de identidad médica.

1. Si la carta dice que quizás le robaron su número del Seguro Social, vea la sección precedente sobre el robo de números de Seguro Social. Comuníquese también con su compañía de seguros o plan de salud, como se indica en el punto 2 a continuación.

2. Si la carta dice que su número de seguro de salud o de plan de salud quedó expuesto, comuníquese con su aseguradora o plan. Cuénteles sobre la violación y pídales que pongan una nota sobre la misma en sus registros y que marquen su número de cuenta.

3. Inspeccione de cerca sus cartas de Explicación de beneficios para ver si hay algún elemento cuestionable. La carta de Explicación de beneficios viene por correo, en general con un aviso que dice "This is not a bill (Esta no es una factura)". Enumera los servicios médicos recibidos por usted y los demás miembros cubiertos por su plan. Si ve un servicio que no recibió, infórmele a su compañía o plan de seguro. Para obtener más información sobre el robo de identidad médica, lea ***First Aid for Medical Identity Theft: Tips for Consumers*** *(Primeros auxilios para el robo de identidad médica: Consejos para consumidores)* en *www.oag.ca.gov/privacy/info-sheets.*

Para obtener más detalles sobre lo que tiene que hacer si sospecha que se está usando su información para cometer robo de identidad, lea ***Identity Theft Victim Checklist*** (*Lo que*

deben hacer las víctimas de robo de identidad) en *www.oag.ca.gov/idtheft/information-sheets.*

Esta hoja se proporciona con fines informativos y no debe interpretarse como asesoramiento legal ni como la política del estado de California. Si desea obtener asesoramiento sobre un caso en particular, debe consultar con un abogado u otro experto. Esta hoja de información se puede copiar, siempre y cuando (1) no se cambie ni se desvirtúe el significado del texto copiado, (2) se dé crédito al Departamento de Justicia de California y (3) todas las copias se distribuyan sin cargo.

Esta hoja se proporciona con fines informativos y no debe interpretarse como asesoramiento legal ni como la política del Estado de California. Si desea obtener asesoramiento sobre un caso en particular, debe consultar con un abogado u otro experto. Esta hoja de información se puede copiar, siempre y cuando (1) no se cambie ni se desvirtúe el significado del texto copiado, (2) se dé crédito al Departamento de Justicia de California y (3) todas las copias se distribuyan sin cargo.

NOTAS

[1] Truth in Lending Act (Ley de Veracidad en los Préstamos), Código de los Estados Unidos, título 14, sección 1601 y subsiguientes.

[2] Electronic Funds Transfer Act (Ley de Transferencia Electrónica de Fondos), Código de los Estados Unidos, título 15, sección 1693 y subsiguientes.

Kamala D. Harris
Attorney General
State of California

California Department of Justice
Privacy Enforcement and Protection Unit
www.oag.ca.gov/privacy