



San Mateo Medical Center

*A County System of Healthcare*

Processing Center • P.O. BOX 141578 • Austin, TX 78714



00228

JOHN Q. SAMPLE

1234 MAIN STREET

ANYTOWN US 12345-6789

18 de mayo de 2018

Asunto: AVISO DE FUGA DE DATOS

Estimado (a) John Sample:

### **¿Qué fue lo que sucedió?**

Lamentamos informarle que ha ocurrido un caso de fuga de datos de su información personal de salud. El 21 de diciembre de 2017 nos percatamos de esta fuga. Un incidente de seguridad ocurrió por medio de un proveedor externo de tecnología. Desafortunadamente, parte de su información personal estuvo involucrada en este incidente.

Nuestro proveedor de tecnología proporciona servicios de transcripción de expedientes médicos para San Mateo Medical Center (SMMC). Recientemente, recibimos una notificación de nuestro proveedor de tecnología que indica que un tercero no autorizado tuvo acceso a determinada información de pacientes. El proveedor de tecnología permite que SMMC genere estos informes para ayudarnos a proporcionar el mejor servicio posible. El proveedor de tecnología contrato a la compañía CrowdStrike, la cual es una empresa líder en seguridad cibernética, para realizar una investigación. La investigación determinó que un tercero no autorizado tuvo acceso a la información de pacientes entre el 20 de noviembre y el 9 de diciembre de 2017. El proveedor de tecnología retiró inmediatamente el sistema afectado después de descubrir este hecho.

El proveedor de tecnología concluyó que existe un riesgo mínimo de que su información se haya visto comprometida. Al parecer, la persona no autorizada no usó, vendió o transfirió esta información.

### **¿Qué tipo de información se incluye en los informes?**

Es posible que la información accedida por un tercero no autorizado incluya la siguiente información: el nombre del paciente, fecha de nacimiento, edad, sexo, número de seguro social, número de expediente médico, número de cuenta del paciente, texto de transcripción médica, así como la fecha de servicio al paciente.



01-05-2-00

### **¿Que estamos haciendo al respecto?**

Estamos trabajando en conjunto con nuestro proveedor de tecnología para resolver este asunto. El proveedor de tecnología también informó a las autoridades sobre este incidente. Como precaución adicional, nuestro proveedor ha solicitado que la compañía AllClear ID proteja su información de identidad durante 24 meses sin costo alguno para usted. Los siguientes servicios de protección de fraude de identidad tienen vigor a partir de la fecha de este aviso y usted podrá acceder a estos servicios en cualquier momento durante los próximos 24 meses.

AllClear Identity Repair: este servicio se encuentra disponible automáticamente sin necesidad de inscribirse. Si surge algún problema, solo tiene que comunicarse al teléfono 1-855-803-1476 y un investigador especializado le ayudará a recuperar las pérdidas financieras, restaurar su crédito y confirmar que su identidad continúe en buen estado.

AllClear Fraud Alerts with Credit Monitoring: este servicio ofrece la posibilidad de establecer, renovar, o eliminar alertas de fraude en su expediente crediticio dentro de un período de 90 días para ayudar a protegerlo en caso de fraude crediticio. Además, le proporciona servicios de supervisión de crédito, un reporte anual de su puntuación de crédito, un informe crediticio y una póliza de seguro de \$1 millón de dólares en caso de fraude de identidad. Para menores de 18 años, AllClear ID ChildScan localiza actos fraudulentos en contra de menores al tener acceso a miles de registros públicos para el uso de la información del menor. Para recibir este servicio, usted necesita proporcionar su información personal a AllClear ID. Usted puede inscribirse en línea al sitio web: [enroll.allclearid.com](http://enroll.allclearid.com), o por vía telefónica al 1-855-803-1476, use el siguiente código de acceso: Redemption Code.

Tenga en cuenta que una vez que usted se inscriba, tiene que seguir algunos pasos adicionales para activar sus alertas telefónicas y alertas de fraude, así como el acceso a su puntuación de crédito y expediente crediticio. Es posible que tenga que seguir algunos pasos adicionales para activar todas las opciones de supervisión de crédito.

### **Usted puede hacer lo siguiente:**

Guarde una copia de este aviso como constancia en caso de que más adelante surja algún problema con su expediente médico. También se recomienda que revise periódicamente el informe que le envía su compañía de seguro médico sobre Aclaración de Prestaciones (EBO, por sus siglas en inglés).

Si usted nota algún servicio que no haya recibido, comuníquese por favor al número de teléfono de la compañía de seguro médico que aparece en el informe. Si usted no recibe un informe completo de aclaración de prestaciones, comuníquese con representante de su plan de salud y solicite que le envíen estos informes cada vez que le proporcionen un servicio a su nombre o con el número de identificación de su plan de salud.

Se recomienda que revise periódicamente sus estados de cuenta y también solicite un informe de crédito de una o más agencias de informes crediticios. Revise por favor el “Ayuda en caso de robo de datos confidenciales”, para recibir información sobre como solicitar un informe de crédito, una suspensión de crédito, alertas de fraude e información adicional sobre protección de robo de identidad.

**Para obtener más información:**

Para recibir información sobre los derechos de privacidad de la información médica, visite el sitio web de California Department of Justice, Privacy Enforcement and Protection, [www.privacy.ca.gov](http://www.privacy.ca.gov). Para recibir información sobre los servicios que se ofrecen, puede comunicarse a AllClear ID al teléfono 1-855-803-1476, de lunes a sábado de 8:00 a.m. a 8:00 p.m. horario del centro del país.

**Comuníquese con nosotros:**

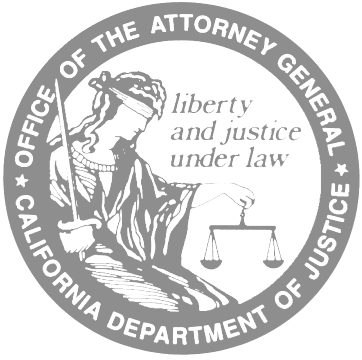
Si tiene preguntas sobre este incidente o si necesita más información sobre qué hacer en casos de fuga de información, por favor no dude en comunicarse con la Directora de Cumplimiento de Normas, Gabriela Behn, al teléfono 1-650-573-2329.

Atentamente,

Gabriela Behn  
Directora de Cumplimiento de Normas y HIPAA







# 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 denúcielas 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.<sup>1</sup>



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 denúcielas 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.<sup>2</sup>
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](http://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](http://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 de 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. Dígalos 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](mailto: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 pídeles 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](http://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](http://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

- <sup>1</sup> Truth in Lending Act (Ley de Veracidad en los Préstamos), Código de los Estados Unidos, título 14, sección 1601 y subsiguientes.
- <sup>2</sup> Electronic Funds Transfer Act (Ley de Transferencia Electrónica de Fondos), Código de los Estados Unidos, título 15, sección 1693 y subsiguientes.



