

September 20, 2013

«Insert Address»

Dear «Insert Name»,

Le estamos escribiendo debido a un incidente reciente en el cuál una computadora del condado fue afectada.

Una computadora del Condado de Monterey que estaba conectada al circuito del Estado de California fue interceptada la noche del 17 de marzo 2013 por usuarios no autorizados en el extranjero quienes estuvieron tratando de entrar al circuito. Esta computadora contenía información sobre individuos que recibieron asistencia pública por medio del Departamento de Servicios Sociales en el Condado de Monterey entre los años 2002 y 2009. Esta información incluía lo siguiente:

Nombre y Apellido
Número de Identificación de Medi-Cal
Dirección
Fecha de Nacimiento

Tan pronto como el Condado recibió la información en marzo 18, 2013 sobre los usuarios no autorizados que trataron de tener acceso a la computadora, la computadora fue desconectada del circuito con el propósito de asegurarla de futuros intentos. Además, administradores del circuito estatal tomaron acción para prevenir intentos similares de acceso no autorizado.

Se hizo una investigación sobre este incidente para determinar si alguna información confidencial en la computadora estuvo expuesta. La investigación concluyó que los usuarios no autorizados pudieron entrar a través de la clave de protección de la computadora entre las fechas de 3/17/2013 y 3/18/2013. Aunque no hemos podido determinar si los datos en la computadora fueron encontrados y transferidos por los usuarios no autorizados, existe la posibilidad de que la información personal fue interceptada.

Hemos informado a la oficina del Procurador de Justicia del Estado de California y a la Oficina Estatal de Protección de Privacidad sobre este incidente. Debido al tipo de información personal en la computadora, recomendamos que considere tomar las siguientes medidas de precaución.

MEDIDAS DE PRECAUCION RECOMENDADAS:

1) Poner un Aviso de Fraude y checar su reportes de crédito. Pudiera poner un aviso de fraude en sus records de crédito y pedir una copia de sus reportes de crédito sin costo para Usted

siguiendo los pasos indicados en el documento adjunto a esta carta titulado:
Recomendaciones Sobre Protección a su Privacidad (Privacy Protection Recommendations).

2) Seguir revisando sus reportes de crédito, checar periódicamente sus estados de cuenta financieros por la posibilidad de robo de identidad. Si Usted descubre actividad sospechosa en sus reportes de crédito, siga las instrucciones en el documento adjunto.

3) Guarde una copia de esta carta para sus records. Es importante para Usted saber que la información personal posiblemente expuesta es solamente la descrita arriba. Aquí están listados los números de las principales oficinas de crédito:

Trans Union -1-800-680-7289

Experian -1-888-397-3742

Equifax - 1-800-525-6285

Información adicional sobre recomendaciones para la protección de privacidad está incluida en el documento adjunto. Para más información sobre robo de identidad, visite el sitio en la red: Oficina de California para asuntos sobre Protección a su Privacidad (California Office of Privacy Protection) en www.privacy.ca.gov.

Lamentamos lo ocurrido y queremos asegurarle que estamos revisando y corrigiendo nuestros procedimientos y prácticas para disminuir el riesgo de que algo semejante pudiera ocurrir con alguna otra computadora ó servidor de archivos. Si necesita más información acerca de este incidente, el Departamento de Servicios Sociales ha designado un número de teléfono gratuito para este propósito. El número es: (855) 670-9850.

Sincerely,



Elliott Robinson
Director

Adjunto [Recomendaciones Sobre Protección a su Privacidad]



Cómo proteger su privacidad

Qué hacer si su información personal está comprometida

Póngase en contacto con las tres agencias de crédito.

- 1** Para informar el robo potencial de su identidad llame sin cargo a cualquiera de las tres agencias principales de crédito indicados a continuación. Accederá a un sistema telefónico automatizado para informar fraude el cual le permitirá marcar su archivo de crédito en las tres agencias de crédito con un alerta de fraude. También le enviarán instrucciones para solicitar una copia de su informe de cada una de las agencias de crédito. No tendrá que pagar por las copias del informe ya que se trata de un posible robo de identidad.

Trans Union 1-800-680-7289

Experian 1-888-397-3742

Equifax 1-800-525-6285

Qué quiere decir poner un alerta de fraude en su archivo de crédito.

- 2** Un alerta de ayudará a protegerlo contra la posibilidad de que un ladrón de identidad abra cuentas nuevas de crédito en su nombre. Cuando un comerciante verifica el historial de crédito de una persona que está solicitando crédito, recibirá un aviso indicando que puede haber fraude en la cuenta. Esto alerta al comerciante a que tome pasos para verificar la identidad del solicitante. El alerta de fraude dura 90 días y se puede renovar.

Examine sus informes de crédito. Revise cuidadosamente cada uno de ellos.

- 3** Fíjese si hay cuentas que no reconoce, sobre todo cuentas abiertas recientemente. Fíjese en la sección de consultas para ver si hay empresas a las que no les solicitó crédito. Algunas empresas facturan bajo un nombre distinto que el nombre de la empresa. En esos casos, la agencia de crédito podrá aclarar de qué empresa se trata. Puede encontrar ciertas consultas identificadas como "promocionales". Estas consultas son efectuadas cuando una compañía obtuvo su nombre y dirección de una agencia de crédito y le envía una oferta de crédito. Las consultas promocionales no son un signo de fraude. (Cuando haga un alerta de fraude, lo eliminarán automáticamente de las listas de ofertas no solicitadas de este tipo). Como precaución general, fíjese también en la sección sobre información personal para ver si hay alguna dirección donde nunca ha vivido.

Si encuentra en su informe transacciones que no comprende, llame a la agencia de crédito al número que aparece en el informe.

- 4** El personal de la agencia de crédito analizará el informe junto con usted. Si no puede explicar la información usted tendrá que llamar a los acreedores involucrados e informar el delito en su comisaría u oficina del alguacil local. Para obtener más información sobre lo que tiene que hacer en este caso, visite el sitio Web de la Oficina de Protección de Privacidad de California en www.privacy.ca.gov y vaya a la página de Robo de identidad (*Identity Theft*).