

**Información Acerca del Incidente de Seguridad  
Que Involucra el Extravío del Dispositivo de Almacenamiento  
Preguntas Frecuentes: [www.childsup.ca.gov](http://www.childsup.ca.gov)**

**1. ¿Qué sucedió?**

El 12 de marzo del 2012, El Departamento de Manutención de Menores (DCSS por sus siglas en inglés) fue notificado por la Oficina de Servicios de Tecnología de California (OTech por sus siglas en inglés) que los dispositivos de almacenamiento computarizados se extraviaron al ser transportados por Federal Express de IBM a Iron Mountain. Los dispositivos de almacenamiento se habían enviado a las instalaciones de IBM en Colorado para una operación de recobrar información en caso de desastre. En este momento no creemos que los artículos extraviados hayan sido entregados a Iron Mountain.

**2. ¿Cuándo sucedió?**

El 12 de marzo del 2012 se nos notifico que faltaban los dispositivos de almacenamiento. El 20 de marzo del 2012 se confirmo que los dispositivos contenían información personal. Desde entonces hemos estado trabajando para identificar a las personas que podrían ser afectadas por este incidente. Adicionalmente, estamos trabajando en conjunto con nuestros proveedores de servicio para tratar de encontrar estos dispositivos – que aun es una posibilidad. No obstante, nuestra meta principal ha sido notificar a toda persona lo más pronto posible. Por esa razón, el 29 de marzo del 2012 se le envió una carta notificando a todas las personas que han sido impactadas por esta situación. Si se recuperan los dispositivos les proveeremos información actualizada.

**3. ¿Porque tienen mi información personal?**

Su información personal es necesaria para conducir las actividades de establecer y hacer cumplir la orden de su caso de manutención.

#### **4. ¿Que información personal fue afectada?**

Los documentos y formas que estaban en los dispositivos contenían una o más de la siguiente información.

- Nombre y domicilio
- Número de seguro social
- Número de licencia de conducir o número de identificación
- Nombre del proveedor de cobertura medica
- Número de identificación del plan medico
- Información del empleador

La información individual de cada participante podría variar dependiendo en que formas y documentos fueron procesados para el caso.

#### **5. ¿Cómo pueden prevenir que esto suceda en el futuro?**

OTech esta trabajando con sus contratistas para mejorar las practicas de seguridad informativas y también esta tomando medidas para establecer nuevos sistemas y procesos para que en el futuro se elimine la necesidad de transportar los dispositivos de almacenamiento.

#### **6. ¿Esto quiere decir que soy victima de robo de identidad?**

No, el hecho que alguien haya tenido acceso a su información no quiere decir que es una victima de robo de identidad o que su información será utilizada para cometer fraude. Hasta ahora no tenemos ninguna razón para creer que alguien haya tenido acceso a su información o la haya utilizado de una manera indebida.

Queríamos notificarle respecto al incidente para que usted pueda tomar los pasos apropiados para protegerse. La manera de protegerse es pedir que se coloque un alerta en su registro de crédito, pedir una copia de su reporte de crédito, y revisarlo para poder detectar posibles problemas.

**7. ¿Qué puedo hacer para proteger mi información personal?**

Se le envió información, adjunto con la primera carta que le enviamos, explicándole los pasos que debe tomar para poner un alerta de fraude en sus registros de crédito. Adicionalmente, puede visitar el sitio web [www.privacy.ca.gov](http://www.privacy.ca.gov) para más información acerca de como proteger su privacidad. También recomendamos que revise regularmente las actividades en sus cuentas de tarjeta de crédito y reporte cualquier actividad fraudulenta a su acreedor.

**8. ¿Qué debo hacer para proteger la información personal de mi hijo?**

En el sitio web de la Oficina de Protección de su Privacidad (*Office of Privacy Protection*) [www.privacy.ca.gov](http://www.privacy.ca.gov) usted encontrará la información acerca de los pasos que debe tomar cuando la información personal de su hijo ha sido comprometida o puede llamar a *Office of Privacy Protection* al 866-785-9663 para asistencia.

**9. ¿Cómo me notificarán si encuentran los dispositivos de almacenamiento?**

Proveeremos información actualizada en nuestro sitio web [www.childsup.ca.gov](http://www.childsup.ca.gov) con cualquier información que se vaya desarrollando.

**10. ¿Cómo sabré si alguien más ha usado mi información personal?**

La mejor manera es ordenando sus reportes de crédito de las siguientes agencias: Equifax, Experian y Trans Union. Si usted descubre cuentas que usted no abrió o solicitudes para crédito (*"inquiries"*) que usted no sometió, estas pueden ser indicaciones de que alguien más puede estar usando su información personal sin su permiso.

También revise regularmente los estados de cuenta que explican los servicios que recibió del seguro medico. Si ve servicios que usted cree no haber recibido, por favor comuníquese con su proveedor de seguro médico al número de teléfono en el estado de cuenta.

**11. ¿Tengo que pagar por el reporte de crédito?**

No. Una vez al año usted puede pedir su reporte de los tres departamentos de crédito sin costo alguno. Usted puede hacer esto visitando el sitio web [www.annualcreditreport.com](http://www.annualcreditreport.com) o por teléfono llamando al 1-877-322-8228.

**12. ¿Que más puedo hacer para protegerme?**

Puede poner un alerta de fraude en sus registros de crédito sin costo alguno. Simplemente llame a uno de los tres departamentos de crédito a uno de los siguientes números y siga las instrucciones de “víctima de fraude”. El primer departamento que usted llame notificará a los otros departamentos para que coloquen el alerta. Cuando llame a la línea de fraude del departamento de crédito se le pedirá información para identificarse y se le dará la oportunidad de proveer un número de teléfono para que los acreedores se comuniquen con usted. Se recomienda que use su número de teléfono celular.

- Trans Union – 1-800-680-7289
- Experian – 1-888-397-3742
- Equifax – 1-800-525-6285

(Aviso: Estos números de teléfono solamente tienen servicio automatizado en inglés)

**13. Llamé a la línea de fraude del departamento de crédito y me pidieron mi número de seguro social. ¿Esta bien dárselo?**

Los departamentos de crédito le piden su número de seguro social y otra información para identificarlo y evitar enviar su reporte de crédito a la persona equivocada. Esta bien proveer ésta información al departamento de crédito siempre y cuando usted haya iniciado la llamada a uno de los números de teléfono gratuitos que le proporcionamos.

**14. ¿Es necesario llamar a los tres departamentos de crédito?**

No. Si usted llama a uno de los departamentos, éste notificará a los otros. Un alerta de fraude se colocará en su registro con los tres departamentos y recibirá una carta de cada departamento confirmando el alerta.

**15. ¿Porqué no puedo hablar con un representante de los departamentos de crédito?**

Primero tiene que solicitar su reporte de crédito para determinar si existe posible fraude. Cuando reciba sus reportes cada uno tendrá un número de teléfono a donde usted podrá llamar y hablar con un representante en la unidad de fraude. Si al revisar su reporte usted encuentra algo inusual o que no comprende, llame al número que aparece en el reporte.

**16. ¿Qué es un alerta de fraude?**

El alerta de fraude es una notificación que los acreedores reciben cuando una persona solicita crédito a su nombre. La notificación alerta a los acreedores que existe la posibilidad de fraude en su cuenta. Los acreedores deberán tomar precauciones para verificar la identidad del solicitante. Por ejemplo, ellos le pueden llamar por teléfono al número que usted proporcionó al pedir el alerta de fraude.

**17. ¿El alerta de fraude me impedirá usar mis tarjetas de crédito?**

No. El alerta de fraude no le impedirá usar sus tarjetas de crédito u otras cuentas. Es posible que demore en recibir nuevas líneas de crédito. El propósito del alerta es protegerlo en contra de un ladrón de identidad que intente abrir líneas de crédito a su nombre. Los acreedores reciben una notificación especial que les alerta que existe la posibilidad de fraude. Los acreedores saben que deben re verificar la identidad de la persona que esta solicitando la línea de crédito.

**18. ¿Cuánto tiempo permanece el alerta de fraude?**

El alerta inicial permanece por 90 días. Si usted quiere renovar el alerta después de los 90 días, lo puede hacer gratuitamente. Adicionalmente, puede remover el alerta al llamar al departamento de crédito al número que aparece en su reporte de crédito.

**19. ¿Qué sucede si coloco el alerta y deseo solicitar una línea de crédito?**

Usted aún puede recibir líneas de crédito. El alerta puede causar que se demore el proceso de la solicitud. Usted puede comprobar su identidad a los acreedores al proveer información de su identidad.

**20. ¿Cuánto tiempo demora el recibir mi reporte de crédito?**

Si usted ordena su reporte utilizando el sitio web [www.annualcreditreport.com](http://www.annualcreditreport.com) usted puede revisarlo por internet. Si lo ordena por teléfono, lo recibirá entre 5 a 10 días.

**21. ¿Debo comunicarme con la Administración de Seguro Social y pedir que cambien mi número de seguro social?**

Rara vez la Administración de Seguro Social otorga cambios de números de seguro social. El simple hecho que exista la posibilidad de uso fraudulento de su seguro social no amerita el cambio. El cambiar el número de seguro social puede tener desventajas. La ausencia de historial de crédito bajo un nuevo número de seguro social le puede causar dificultades en obtener líneas de crédito, continuar con sus estudios de colegio, alquilar un apartamento, abrir cuentas bancarias, obtener seguro medico, etc. En la mayoría de los casos no es recomendable cambiar el número de seguro social.

**22. ¿Debo cerrar mi cuenta bancaria?**

No, al menos que su número de cuenta bancaria fue uno de los datos comprometidos por la violación de seguridad. Como medida general para la protección de su privacidad, usted debe limitar el uso del número de seguro social cuando no es requerido. Si el número de identidad personal (PIN por sus siglas en inglés) de su cuenta bancaria es su número de seguro social usted debe pedirle a su banco un PIN diferente. NO utilice los últimos cuatro números de su seguro social, su apellido materno, o su fecha de nacimiento como clave para transacciones financieras.

**23. ¿Debo cancelar mis tarjetas de crédito u otras cuentas?**

No, al menos que su número de cuenta fue uno de los datos comprometidos por la violación de seguridad. Como medida general para la protección de su privacidad, usted debe revisar su estado de cuenta cuidadosamente para determinar si existen cargos que usted no hizo. Si es así, comuníquese con el acreedor inmediatamente.

**24. ¿Qué debo buscar en mi reporte de crédito?**

Busque cuentas que no reconoce, especialmente cuentas recientemente abiertas. Examine la sección de solicitudes e indagaciones de las cuales usted no ha solicitado línea de crédito. Cabe notar que ciertos tipos de indagaciones anotados como “*promotional inquiries*” son para ofertas de crédito no solicitadas, y la mayoría son de compañías con las cuales usted hace negocios.

No considere estas indagaciones como señal de fraude. Si usted tiene un alerta de fraude, será automáticamente eliminado de las listas que lo someten a ofertas pre aprobadas o puede llamar al 888-5OPTOUT para pedir que lo excluyan.

Busque en la sección de información personal para identificar direcciones donde nunca ha vivido. Cualquiera de estas situaciones puede ser una indicación de fraude. Esté al pendiente de otras señales de robo de identidad tal y como llamadas de acreedores o agencias de colección sobre cobros que no reconoce o cargos inusuales a su tarjeta de crédito.

**25. ¿Qué sucede si descubro que he sido víctima de robo de identidad?**

Usted debe notificar a su departamento local de policía, los acreedores involucrados y los departamentos de crédito. Para más información acerca de lo que debe hacer, vaya al sitio web de la Oficina del Estado de California para Protección a la Privacidad, [www.privacy.ca.gov](http://www.privacy.ca.gov) y seleccione *Identity Theft*, después seleccione el link [Spanish and Chinese, please click here](#) y escoja el número 3. *Identity Theft Victim Checklist* o vaya directamente al siguiente link: <http://www.privacy.ca.gov/consumers/cis2spanish.pdf>

**26. ¿Qué tan seguido y por cuanto tiempo debo continuar pidiendo mi reporte de crédito?**

Por un tiempo podría ser buena idea pedir los reportes de crédito cada tres meses. Por cuanto tiempo usted debe continuar pidiendo los reportes es a su discreción. Usualmente, pero no siempre, los ladrones de identidad actúan enseguida de haber robado información personal. Como medida general para la protección de su privacidad, recomendamos revisar su reporte de crédito por lo menos dos veces al año.

**27. ¿Hay algún número de teléfono a donde puedo llamar para obtener más información sobre mi caso de manutención de menores?**

Si no encuentra la información que necesita en la carta que le enviamos o en la información proveída en esta pagina, puede llamar al (866) 901-7674.

**28. Cuando llamo a los departamentos de crédito, me quieren vender protección de crédito adicional. ¿Es buena idea? ¿Quien debería pagar por esta protección?**

Para este incidente no creemos que sea necesario un servicio de protección de crédito continuo. Para poder tener acceso a la información contenida en las cintas extraviadas se requiere hardware y software de nivel comercial y aun así cada documento contenido en la cinta tendrá que ser examinado individualmente. La probabilidad de que su información personal llegue a manos de un individuo con intenciones de cometer robo de identidad es extremadamente pequeña y prácticamente nula. Por estas razones, no recomendamos que compre protección adicional y el estado de California no puede hacer arreglos para pagar por estos servicios adicionales.

**29. ¿Porqué tardaron tanto para notificarme del incidente?**

Fue importante para nosotros primeramente verificar que las cintas estaban efectivamente extraviadas y no se podían localizar. Segundo, fue importante verificar cuales clientes fueron afectados. Finalmente, tuvimos que hacer arreglos para imprimir y enviar las notificaciones.