ser valiosos, en particular aquellos que sospechan que alguien pudo haber robado información personal, robado información personal, aquellos que no son cuidadosos con la información personal o tienen muchos integrantes de la familia que utilizan las mismas tarjetas de crédito. Los consumidores deben entender exactamente qué es lo que un servicio de protección contra robo de identidad proporciona, antes de suscribirse, ya que algunos de estos servicios se encuentran disponibles de manera gratuita.

Seguro contra robo de identidad: el seguro contra robo de identidad ofrece un reembolso por muchos de los costos relacionados con el hecho de reclamar su identidad y de restablecer su buena reputación. El reembolso puede ser, por ejemplo, por concepto de: servicios postales, cargos legales, o pagos por tiempo utilizado en asuntos relacionados con el robo de identidad. Por medio del seguro no se puede eliminar el daño dejado en su crédito por el robo de identidad; pero puede ayudarlo a que se recupere de este delito. Este seguro se puede obtener por medio de seguros de propietarios de viviendas o inquilinos, como una póliza independiente o mediante una tarjeta de crédito.

La cobertura que brinda este seguro varía mucho entre los aseguradores, por lo tanto, debe comprender exactamente qué es lo que puede estar comprando. Para determinar si debe comprar este seguro, tenga en cuenta que la víctima de robo de identidad promedio paga aproximadamente $1000 en gastos varios para restablecer su identidad, y gasta el equivalente a aproximadamente 20 días de trabajo para limpiar su registro. Debe considerar el beneficio que esta cobertura pueda representar para usted. El hecho de que su empleador puede ser que no autorice los permisos sin salario, la cobertura del seguro le convendría, ya que esta puede que le cubra el monto del salario que corresponde al tiempo perdido. Sin embargo, también debe saber que sólo el 16% de las víctimas necesitan asesoramiento legal para anular sentencias e informes delictivos sobre delitos cometidos a nombre de la victima de estos ladrones. Algunos emisores de tarjeta ponen a disponibilidad de los dueños de tarjeta de crédito asistencia gratuita por robo de identidad.

Los consumidores que compren un seguro contra robo de identidad deberán continuar protegiendo su información financiera personal, ya que el robo de identidad aún puede ocurrir y manchar su crédito.

El mejor seguro es la prevención.

Deciembre 2008

Un Producto del Programa de Prevención y Asistencia del Robo de Identidad de
La Junta de Protección al Consumidor del Estado de Nueva York

Protejiendo y Educando al Consumidor

La Junta de Protección al Consumidor del Estado de Nueva York
Línea Gratis de Ayuda
1-800-697-1220
nysconsumer.gov

David A. Paterson
Gobernador

Mindy A. Bockstein
Presidenta y Directora Ejecutiva

Una Guía para Consumidores para Prevenir y Responder al

ROBO de IDENTIDAD

ROBO de IDENTIDAD

LA JUNTA DE PROTECCIÓN AL CONSUMIDOR DEL ESTADO DE NUEVA YORK
PROTEJIENDO Y EDUCANDO AL CONSUMIDOR
NYSCONSUMER.GOV
1-800-697-1220

UN PRODUCTO DEL PROGRAMA DE PREVENCION Y ASISTENCIA DEL ROBO DE IDENTIDAD DE LA JUNTA DE PROTECCION AL CONSUMIDOR DEL ESTADO DE NUEVA YORK

INTRODUCCIÓN

El robo de identidad es el reclamo de fraude más común por parte de los consumidores y es el delito financiero de más rápido crecimiento, afectando aproximadamente de 8 a 15 millones de estadounidenses por año. Es de especial preocupación en Nueva York, ya que este estado tiene el sexto índice per cápita de robo de identidad más alto del país. Algunas víctimas de robo de identidad han perdido oportunidades laborales, otorgamientos de préstamos o han sido arrestadas por delitos que no cometieron. A las víctimas de robo de identidad les lleva un promedio de dos años y miles de dólares resolver los problemas causados por robo de identidad.

El robo de identidad se produce cuando los ladrones utilizan información personal tal como la fecha de nacimiento, dirección, número de seguro social, números de teléfono, número de tarjetas de crédito y de cuentas bancarias y contraseñas. Los delincuentes pueden entonces abrir nuevas cuentas a nombre de la victima, solicitar préstamos, hacer grandes compras, vaciar sus cuentas bancarias y adquirir sus activos.

El robo de identidad les cuesta a los consumidores y a las compañías más de $50 mil millones por año.

Cualquiera puede ser víctima del robo de identidad, incluso los niños. A menudo, los padres no solicitan un informe de crédito ni tampoco un informe de "no actividad" a las agencias de informe de crédito para realizar un control, ni toman las medidas necesarias para garantizar que la información personal de sus hijos esté a salvo. Como consecuencia, muchos jóvenes se sorprenden al descubrir que alguien les robó la identidad y arruinó su crédito, incluso antes de tener la posibilidad de utilizar su primera tarjeta de crédito. Frecuentemente, el robo de identidad lo comete una persona que usted conoce.

CÓMO SE PRODUCE EL ROBO DE IDENTIDAD

Unas de las formas más comunes en las que los delincuentes pueden robar información personal son: tomar correspondencia que usted tiró a la basura; obtener información personal de compañías al robar los registros o acceder, sin autorización a la información contenida en computadoras, y extraer información de usted de manera engañosa al hacerse pasar por personal del banco, una compañía legítima o un funcionario del gobierno.

Señales de advertencia

Desafortunadamente, en muchos casos es difícil probar que se produjo un robo de identidad. Sin embargo, debe preocuparse si:

- recibe facturas por compras que nunca realizó o notificaciones de cobro relacionadas con deudas en las que nunca incurrió.

4. Llame al Centro de Intercambio de Información de Robo de Identidad al 1-877-438-4338 para informar el robo. La Comisión Federal de Comercio administra y mantiene el Centro de Intercambio de Información. Los asesores le brindarán asesoramiento adicional. El Centro de Intercambio de Información les brinda a los oficiales de oficinas policiales una base de datos central de reclamos de robo de identidad.

5. Si le roban o pierde cheques personales, notifique inmediatamente al banco y solicite que se coloque una "detención de pago" en todos los cheques reportados. Pídale al banco que notifique a la compañía de verificación de cheques que ellos utilizan. Hay varias compañías que provean verificación de cheques. Los siguientes son las compañías principales (ese no es un lista completa):

Certegy Check Services:	1-800-437-5120
ChexSystems:	1-800-428-9623
CrossCheck:	1-800-552-1900
(tenga a mano el número de la tienda cuado llame)	
Network (SCAN):	1-800-262-7771
TeleCheck:	1-800-710-9898

6. Si le han robado la licencia de conducir o cualquier otro tipo de identificación emitida por el gobierno, comuníquese con la agencia que emitió dicho documento. Siga los procedimientos para cancelar y obtener un reemplazo. Comuníquese con el Servicio Postal de Estados Unidos si sospecha que el ladrón de identidad utilizó el correo.

7. Si usted es jubilado o minusválido, puede que reúna los requisitos para recibir una compensación que cubra los gastos generados por asesoramiento financiero por ser víctima de un delito. Esto lo otorga la Junta de Víctimas de Delitos del Estado de Nueva York (CVB por las siglas en inglés). Comuníquese con la CVB al: 1-800-247-8035.

SERVICIOS DE PROTECCIÓN DE IDENTIDAD Y SEGURO CONTRA ROBO DE IDENTIDAD

Existen productos y servicios disponibles para ayudarlo a proteger su identidad, y a compensarlo por los gastos que pueda tener para solucionar los problemas causados por el ladrón, esto es en caso de haber sido victima de robo de identidad.

Servicios de protección contra el robo de identidad: estos servicios le ayudan a identificar rápidamente cualquier cambio en el informe de crédito, haciendo más fácil detectar el robo de identidad. Generalmente proporcionan un monitoreo del informe de crédito todos los días hábiles, proporcionan informes trimestrales de los cambios en el informe de crédito y le proporcionan copias de su informe de crédito. Para muchos consumidores estos servicios podrían

QUÉ DEBE HACER EN CASO DE SER VÍCTIMA DE UN ROBO DE IDENTIDAD

1. Comuníquese con el departamento de fraude de las tres principales agencias de informe de crédito:

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

   Infórmeles que robaron su identidad y solicite que se ponga una "alerta de fraude" en su expediente. Esta alerta puede prevenir que alguien abra cuentas nuevas a su nombre. También pida copias gratuitas del informe de crédito y revíselo cuidadosamente para identificar cuentas o cargos no autorizados.

   Existen dos tipos de alerta de fraude:

   - alerta inicial: permanece en el informe de crédito por al menos 90 días. Esto es apropiado si sospecha que ha sido, o está por ser, víctima de robo de identidad. Cuando coloca una alerta de fraude inicial en el informe de crédito, usted tiene derecho a un informe de crédito gratuito.
   - alerta extendida: permanece en el informe por 7 años. Esto es apropiado si ha sido víctima de robo de identidad y usted le proporciona a la compañía de informe de crédito un "informe de robo de identidad." Cuando coloca una alerta extendida en el informe de crédito, usted tiene derecho a obtener dos informes de crédito gratuitos emitidos por cada una de las tres compañías principales de informe de crédito, dentro de un periodo de 12 meses . Cuando una compañía ve la alerta en el informe de crédito, debe verificar su identidad antes de otorgar un crédito.

2. Comuníquese con el departamento de seguridad del acreedor o de la institución financiera y haga un seguimiento por escrito por cada cuenta que se abrió o a la que se accedió fraudulentamente. Cancele inmediatamente las cuentas manipuladas y abra cuentas nuevas que requieran contraseñas para poder acceder.
3. Presente un informe en el departamento de policía. El robo de identidad y el fraude son delitos penados por la ley. Guarde una copia del informe policial para presentar ante las compañías de tarjetas de crédito, bancos y agencias de informe de crédito como prueba de que se cometió un delito. El hecho de entregar un informe policial puede bloquear el informe de datos fraudulentos en su informe de crédito.

- se le niega un crédito sin razón aparente.
- deja de recibir estados de cuenta mensuales del banco o de las tarjetas de crédito.
- el informe de crédito contiene información incorrecta.

CÓMO PROTEGERSE

Puede reducir el riesgo de convertirse en una víctima de robo de identidad si maneja su información personal cuidadosa y cautelosamente.

Proteja su información personal

- Mantenga su información personal en un lugar seguro. Guarde esta información en un lugar que no esté a la vista, especialmente si contrata ayuda externa para trabajar en su casa, o si tiene compañeros de cuarto.
- Minimice el uso de su número de seguro social. Proporcione el número de seguro social sólo cuando sea absolutamente necesario. Pida que se utilice otro número de identificación siempre que sea posible. Cuando le envíe un pago a un acreedor, no ponga el número de seguro social ni el número de teléfono en el cheque. En el Estado de Nueva York es ilegal que una compañía pida los números de cuenta o el número de seguro social en un cheque. Nueva York también prohibe su número de seguro social de ser utilizado como una identificación personal, una contraseña o un código en una carta de asociación o servicio. Una entidad no le puede requerir a transmitir su número de seguro social sobre el Internet a menos que la conexión sea segura o el número de seguro social es cifrado. Es también ilegal para cualquiera revelar intencionalmente su número de seguro social.
- Verifique regularmente la declaración de beneficios médicos. Le pueden haber robado y utilizado la información de la cuenta médica.
- Limite la información que lleva en la billetera. Lleve sólo las tarjetas de crédito que planea utilizar y solamente lleve la tarjeta de seguro social si es absolutamente necesario. Haga copias y/o una lista de todo lo que contenga información personal en su billetera.
- Determine cómo se utilizará la información personal. Antes de dar a conocer información personal, averigüe cómo se utilizará y con quién se compartirá dicha información. Hágale saber a las compañías que quiere que su información personal no se comparta con nadie más.
- Coloque contraseñas en la tarjeta de crédito y en las cuentas bancarias y de teléfono. Evite utilizar contraseñas comunes o números de identificación personal (PIN) tales como el apellido de soltera de su madre, su fecha de nacimiento o número de teléfono.

- Desháguese correctamente de los documentos. Triture o queme cualquier documento que contenga información personal. Asegúrese de destruir las tarjetas de crédito preaprobadas.

- Minimice el uso de correo electrónico para actividades bancarias. Utilice el depósito directo y recoja los cheques personales del banco siempre que sea posible. Esto reducirá la probabilidad de que la información de cuenta y cheques personales caigan en manos equivocadas.

- Proteja su correo del robo. Deposite el correo saliente en las casillas de recolección del correo o en la oficina postal, y no en casillas de correo inseguras. Quite el correo de su casilla rápidamente.

- No pierda de vista su tarjeta de crédito. Los ladrones pueden utilizar lectores de tarjetas magnéticas portátiles para extraer información personal de la banda magnética de las tarjetas de crédito o débito. Entre los inculpados se incluyen mozos, empleados de estaciones de servicio y tiendas.

- Sea cuidadoso cuando utilice cajeros automáticos (ATM). Cuando esté en un ATM, tenga precaución y desconfíe de la gente a su alrededor. Se pueden utilizar teléfonos celulares para tomar una fotografía del ATM o de la tarjeta de crédito. Si un ATM está en un lugar cerrado, trate de ser el único que se encuentre adentro. Además, intente utilizar sólo ATM asociados a bancos. Se han improvisado algunos ATM privados o independientes para permitirles a los ladrones robar números de cuenta y códigos de identificación personal (PIN).

- Reduzca los ofrecimientos de tarjetas de créditos no solicitados. Cuanto menos ofrecimientos de tarjetas de crédito reciba, menor es la probabilidad de que le roben una tarjeta de crédito. Llame al 1-888-5OPTOUT y pida que se elimine su nombre de esas listas de comercialización y pida que las instituciones financieras no compartan la información con compañías no afiliadas.

Sea prudente cuando utilice la computadora

- Prevenga el acceso no autorizado a la computadora. Algunos virus pueden hacer que la computadora envíe información a desconocidos. Para ayudar a prevenir esos virus, actualice regularmente su *software* de protección contra virus y no descargue archivos de extraños ni haga clic sobre vínculos de gente que no conoce. Utilice una barrera, especialmente si tiene conexión de internet de alta velocidad o si está siempre conectado a la red.

- Tenga cuidado cuando transmita información personal. Utilice un explorador seguro. Cuando ingrese información personal, busque el icono "bloqueado" en la barra de estado.

- Tenga cuidado con el fraude electrónico, "*phishing*". El fraude electrónico ocurre cuando se envían correos electrónicos masivos o mensajes de ventanas emergentes que engañan a los consumidores para que divulguen sus números de cuenta, contraseñas, números de seguro social y otra información personal. Esto ocurre frecuentemente a través de correos electrónicos que le piden "actualizar" o "validar" registros o cuentas. El mensaje lo puede llevar a un sitio web similar al de una organización legítima pero que en realidad no lo es. Para ayudar a evitar esto, no le proporcione información personal a alguien que lo llame o le envíe un correo electrónico sin que usted lo haya pedido. Las compañías legítimas no solicitan información de esta forma. Por el contrario, primero llame o envíe un correo electrónico a la compañía para confirmar la legitimidad de la solicitud. Comuníquese utilizando la información que para este fin aparece en el estado de cuenta, o use el directorio de teléfono.

  Se crean más de 1000 sitios web de "*phishing*" por mes. La mayoría se desconecta después de sólo 3 días, lo que dificulta que la oficina policial encuentre a los culpables.

- No guarde información delicada en su computadora portátil. Las computadoras portátiles se pueden robar fácilmente. Evite utilizar una función que guarde su nombre de usuario y contraseña en su computadora portátil. Siempre salga del sistema cuando termine.

- Desháguese de las computadoras correctamente. Borre cualquier información personal que haya guardado en su computadora antes de deshacerse de ella. Para esto, utilice un programa de utilidades "eliminación" que sobrescribe el disco duro.

Revise cuidadosamente las facturas e informes de crédito.

- Mantenga registros bien organizados de todas las cuentas bancarias y tarjetas de crédito. Un estado de cuenta que falte puede significar que alguien obtuvo y envió su información financiera a otro lado.

- Revise sus facturas. Antes de enviar un pago, revise cuidadosamente todas las facturas. Los cambios no autorizados pueden ser la primera señal de robo de identidad.

- Revise sus informes de crédito. Si un ladrón de identidad abre cuentas nuevas a su nombre, es probable que estas cuentas aparezcan en el informe de crédito. Los residentes de Nueva York pueden obtener un informe de crédito gratuito de cada una de las tres agencias nacionales de informe de crédito, una vez cada 12 meses. Visite: annualcreditreport.com o llame al 1-877-322-8228 para pedir un informe gratuito. Verifique la precisión del informe de crédito y solicítele a la agencia de crédito que documente y revise cualquier información incompleta o incorrecta.

  Muchos asesores financieros aconsejan obtener un informe de crédito gratuito a la vez, y el resto distribuidos por igual a lo largo del año. Esto puede ayudar a detectar cambios o a verificar información nueva, también permite identificar problemas más rápidamente de lo que hubiera ocurrido de haber solicitado los tres créditos al mismo tiempo.