## SI ES VÍCTIMA DE UN ROBO DE IDENTIDAD

Si detecta un robo de identidad de manera temprana y actúa con celeridad, puede minimizar los daños. Tome las siguientes medidas:

**Lleve un registro diario.** Registre todas las medidas que tome para limpiar su nombre. Incluya los nombres de organismos, empresas e individuos. Lleve registros detallados de las llamadas telefónicas y copias de la correspondencia.

**Presente una declaración jurada sobre el robo de identidad.** Comuníquese con la FTC al (877) 438-4338 o visite www.ftc.gov para presentar una reclamación y crear una declaración jurada sobre robo de identidad. El informe de la policía, junto con la declaración jurada, será el **informe de robo de identidad** que usará para disputar cuentas fraudulentas.

**Presente un informe policial.** Visite la estación de policía y entréguele al oficial que redacte el informe una copia de su declaración jurada sobre robo de identidad FTC y cualquier prueba de robo. Asegúrese de que en el informe de la policía aparezcan todos los informes fraudulentos. Es posible que necesite el informe policial para probar que es la víctima cuando disputa cargos o cuentas fraudulentas.

**Dispute la información fraudulenta de su informe crediticio.** Envíe su informe de robo de identidad a cada agencia de informes crediticios junto con una carta en la que se solicite que se bloquee la aparición de las cuentas fraudulentas en su informe crediticio. (Continúe revisando sus informes crediticios después del hecho, en caso de que vuelva a aparecer información fraudulenta en ellos).

**Comuníquese con sus acreedores.** Notificar a sus acreedores por teléfono y por escrito, por correo certificado que ha sido víctima de un robo de identidad. Incluya una copia del informe de robo de identidad. Solicíteles que dejen de brindar información fraudulenta a las agencias de informes crediticios.

**Comuníquese con su banco.** Denuncie ante el banco los cheques falsificados. Si su cuenta bancaria o su línea de crédito se ve comprometida de alguna forma, incluso cuando crea que el daño es insignificante, notifique al banco, cierre la cuenta por completo y abra una nueva cuenta o línea de crédito. Denuncie las tarjetas de crédito o débito que haya perdido o le hayan robado. Tome medidas rápidamente para limitar su responsabilidad.

**Comuníquese con el DMV.** Si le roban su licencia de conducir, entregue su informe policial al DMV local cuando solicite el reemplazo de su licencia. Pídales que adjunten una copia del informe junto con sus registros. Si tiene pruebas de que otra persona recibió una licencia, un registro o un título de propiedad a su nombre, presente el formulario FI-17 (informe de uso no autorizado de licencia o registro). Es posible que deba cambiar el número de licencia si el ladrón la está usando.

**Comuníquese con las entidades de servicios públicos.** Notifique a las empresas de servicios públicos y de telefonía que usted ha sido víctima de un robo de identidad. Un ladrón de identidad puede tratar de abrir una cuenta nueva en su nombre usando la factura de un servicio público.

**Comuníquese con la Administración de Seguridad Social.** Si sospecha que otra persona está usando su número de Seguro Social, llame a la línea de denuncia de fraudes de la Administración de Seguridad Social al (800) 269-0271 o visite www.ssa.gov/oig. Puede verificar su registro de ingresos llamando al (800) 772-1213.

**Cambie/agregue contraseñas.** Cambie las contraseñas de sus cuentas. Use contraseñas seguras de al menos 8 caracteres que incluyan una combinación de símbolos, números y letras minúsculas y mayúsculas. No use como contraseña palabras que aparecen en el diccionario, secuencias alfabéticas, numéricas o de teclas comunes, ni parte de su número de Seguro Social ni información personal.

## USE UNA ALERTA DE FRAUDE Y UN BLOQUEO DE SEGURIDAD

Si es víctima de un robo de identidad, considere colocar un “bloqueo de seguridad” o una “alerta de fraude” en su archivo en las tres agencias de informes crediticios principales.

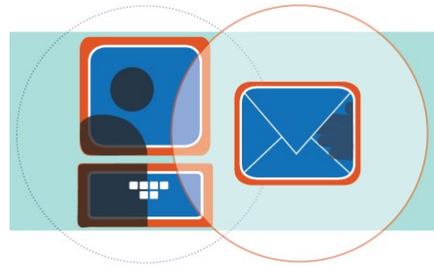
Un **bloqueo de seguridad**, por lo general, impide que los acreedores accedan a sus archivos crediticios, lo que evita que se abran nuevas líneas de crédito, a menos que usted autorice el acceso para las agencias. Los procedimientos para obtener un bloqueo de seguridad varían levemente entre cada una de las tres agencias de informes crediticios, y debe tener un bloqueo distinto para cada una de ellas. Visite sus sitios web (www.equifax.com, www.transunion.com, www.experian.com) para saber cómo hacerlo.

Una **alerta de fraude** advierte a los acreedores para que se comuniquen con usted antes de abrir nuevas cuentas o cambiar las existentes. A diferencia de un bloqueo de seguridad, una alerta de fraude no bloquea su crédito; si bien los acreedores recibirán un mensaje de alerta, no hay garantía alguna de que no emitirán crédito. Una alerta de fraude suele durar 90 días, aunque puede extenderse. Para obtener una alerta de fraude, pídale a una de las tres agencias de informes crediticios que programe una para su informe crediticio. Es necesario que esa agencia les informe a las otras dos agencias, pero usted debe confirmar con la agencia a la que llame si ésta puede notificar a las otras dos. Visite el sitio web de Equifax, TransUnion o Experian para conocer cómo colocar una alerta.

## PIDA AYUDA

Para obtener más información o presentar una reclamación, visite nuestro sitio web en **www.dfs.ny.gov** o llame al **(800) 342-3736**.

NEW YORK STATE OF OPPORTUNITY. Department of Financial Services



*Lo que necesita saber sobre...*

# ROBO DE IDENTIDAD

Esta guía se ofrece con fines informativos solamente y no c onstituye asesoría legal.

***www.dfs.ny.gov***

**(800) 342-3736**

Para que un profesional de extensión del DFS presente un programa sobre el robo de identidad en su organización, comuníquese con James Dees al (212) 480-7246.

Información importante sobre cómo protegerse y qué hacer si es víctima de un robo de identidad.

## ¿QUÉ ES EL ROBO DE IDENTIDAD?

El robo de identidad es la práctica de robar la información personal que identifica a una persona con el propósito de usarla para obtener bienes, beneficios o servicios de forma fraudulenta. Puede ocurrir en línea o fuera de línea.

El robo de identidad puede causar problemas de crédito, así como rechazo a que lo empleen, a acceder a créditos, a que lo aseguren y a obtener licencias profesionales. A menudo, las víctimas dedican mucho tiempo y dinero reclamando para recuperar su buen nombre y su reputación.

## CONSEJOS PARA PROTEGERSE

Usted es la primera línea de defensa para protegerse de robos de identidad. Estas son algunas de las medidas que puede tomar para prevenir el robo de información personal:

**Verifique su informe crediticio.** Revisar los informes crediticios de manera periódica es una buena manera de detectar un robo de identidad a tiempo. Si un ladrón de identidad abre nuevas cuentas a su nombre, es probable que estas aparezcan en su informe. Los neoyorquinos pueden obtener un informe crediticio gratuito de tres agencias de informes crediticios importantes (Equifax, Experian y TransUnion) una vez por año. Visite www.annualcreditreport.com o llame al (877) 322-8228 para obtener estos informes gratuitos. Aproveche este beneficio y solicite un informe de una agencia diferente cada cuatro meses..

**Almacene la información confidencial y deshágase de ella de forma segura.** Conserve su tarjeta del Seguro Social, su certificado de nacimiento y otros documentos e identificaciones importantes en un lugar seguro. Sea cauto respecto del lugar donde deja material privado, como facturas y resúmenes bancarios, y dispositivos digitales que puedan contener material confidencial o información personal de identificación. Antes de eliminar el correo postal, triture los documentos confidenciales. Denuncie cuanto antes las tarjetas de crédito, de débito o de cajero automático que pierda o que le roben.

**Sea consciente de la información que da a conocer.** No es buena idea publicar información personal de identificación en redes sociales ni darlas por teléfono, a menos de que esté seguro de la persona con la que habla. Antes de brindar información personal de identificación, pregunte cómo se usará y se protegerá. Asegúrese de no imprimir su licencia de conducir, su número de Seguro Social, sus números de cuentas u otra información delicada en los cheques o fuera de los sobres de pago o de depósito.

**Utilice los servicios en línea con precaución.** Puede proteger mejor sus cuentas y transacciones en línea usando contraseñas seguras que actualice de forma periódica. Use la autenticación multifactorial si es posible. La autenticación multifactorial exige el uso de más de un método de identificación para verificar la identidad de un usuario. Cuando termine con una sesión segura, recuerde cerrar la sesión por completo. Si realiza una compra en línea, introduzca su información de pago por medio de sitios seguros y cifrados que tengan el icono de un candado en la barra de direcciones y una dirección URL que empiece con https. Para conocer las prácticas de manejo de la información de un sitio, revise las prácticas de privacidad antes de usarlo y considere salir de él si no se siente cómodo con sus prácticas.

Piense dos veces antes de descargar archivos o hacer clic en enlaces o archivos adjuntos inesperados o poco familiares que lleguen por correo electrónico. Dado que el correo electrónico suele ser inseguro, no comunique su número de Seguro Social ni otra información delicada por este medio, ni los trasmita por Internet (a menos que use un sitio seguro y cifrado al que haya ingresado directamente).

Esté atento a los sitios de suplantación de identidad (*phishing)*, sitios fraudulentos que imitan los sitios reales para capturar la información personal de los usuarios. Tenga cuidado si utiliza zonas de WiFi públicas que no son seguras.

**Protéjase al usar cajeros automáticos.** En lo posible, utilice una tarjeta que tenga un chip; la tecnología de chip es más segura. Al usar un cajero automático, tápelo con el cuerpo para evitar que otras personas vean y roben su información personal.

Tenga cuidado y no use cajeros que parezcan inusuales o extraños. Los cajeros privados tienen menos protecciones de seguridad que los cajeros de los bancos.

Tomar su recibo. Puede contener información personal, como el saldo de la cuenta. Antes de dejar el cajero, asegúrese de finalizar la transacción y tener la tarjeta consigo. Por supuesto, nunca dé a conocer su PIN.

**Proteja su computadora y sus dispositivos móviles.** Para lograr la máxima protección, se recomienda que instale un *firewall* en la computadora de su hogar para impedir que los *hackers* obtengan información de identificación personal y financiera de su disco duro; instale y actualice de forma periódica su *software* de protección antivirus para que el *malware* no haga que su computadora envíe archivos u otra información almacenada; también instale parches de seguridad en su navegador de forma periódica.

Si dispone de una red inalámbrica, asegúrese de protegerla con contraseña para acceder a ella. Además, recuerde proteger su computadora, teléfono celular y otros dispositivos de asistencia personal con una contraseña segura.

**Controle la divulgación de información y el correo postal.** Preste atención a los ciclos de facturación y revise sus cuentas de manera regular. Si no recibe las facturas a tiempo, llame a la empresa. (A veces, los ladrones de identidad cambian su dirección de facturación o desvían su correo postal).

Es buena idea limitar la recepción de correspondencia privada siempre que sea posible, a fin de evitar la posibilidad de un robo. Si planifica no estar en su casa durante un período largo, llame al Servicio Postal de los EE. UU. y solicite el servicio para que le retengan su correspondencia. Además, los consumidores pueden solicitar que se quite su nombre de las listas de *marketing* y optar por no recibir ofertas no deseadas de crédito llamando al 888-567-8688. Esta decisión reducirá la cantidad de correspondencia de ofertas que usted recibe.

**Limite lo que lleva consigo.** Tome medidas para minimizar su exposición al robo de identidad en caso de que pierda o le roben la cartera; para ello, solo lleve consigo las tarjetas de crédito y débito que realmente necesita. Además, algunas de las tarjetas de beneficios médicos y de farmacia pueden contener su número de Seguro Social. Si es así, solo llévelas cuando necesite usarlas.

Es buena idea memorizar los números de identificación personal (como el PIN del cajero automático) y las contraseñas en línea, en lugar de tenerlas en su cartera o bolso.

**Proteja su número de Seguro Social.** Su número de Seguro Social es un dato personal importante que muchas entidades usan como identificación para la declaración de impuestos, cuestiones laborales, informes crediticios y otros fines. Tome medidas para estar seguro de que no caiga en malas manos.

Cuando una persona le solicite su número, pregunte por qué lo necesita y si se puede usar una identificación alternativa. No se recomienda que brinde su número de Seguro Social en cheques, por teléfono en público, como forma de identificación general, al efectuar una compra en una tienda o por correo electrónico.

Por lo general, los empleadores, las instituciones financieras (bancos, cooperativas de crédito, compañías de seguros) y el Servicio de Impuestos Internos (y otras entidades de recolección de impuestos) pueden solicitar legítimamente su número de Seguro Social.

**Proteja su información médica.** Un ladrón de identidad puede usar el nombre o la información del seguro médico de la víctima para obtener atención médica o recetas, o presentar reclamaciones ante una compañía de seguros.

Siempre recuerde controlar toda la correspondencia, los correos electrónicos y los registros relacionados con su salud, y revisar los informes contables y las comunicaciones de su compañía de seguros y de los proveedores de atención médica, a fin de detectar elementos y servicios inusuales y afecciones que usted no tenga. Notifique a la compañía de seguros y al proveedor en caso de que detecte un error.

**Proteja la información médica de su hijo.** El crédito de un menor es muy valioso para un ladrón de identidad. Proteja la información personal de su hijo y asesórelo en cuanto a la seguridad en línea.