

- Si se ha otorgado un Préstamo Estudiantil a su nombre en forma fraudulenta

Si un delincuente ha solicitado un préstamo estudiantil a su nombre, debe cerrar el préstamo comunicándose con la escuela o el programa que lo abrió. También informe sobre el préstamo fraudulento al Departamento de Educación de los Estados Unidos al teléfono 800.mis.used, o en línea a www.ed.gov/offices/oig/hotline.htm, o por correspondencia a la Oficina del Inspector General, Departamento de Educación de los Estados Unidos (Office of Inspector General, U.S. Department of Education), 400 Maryland Avenue, SW, Washington, DC 20202-1510.

- Si se ha presentado una declaración jurada impositiva a su nombre en forma fraudulenta

Si un delincuente está presentando declaraciones juradas impositivas a su nombre, diríjase al Servicio de Impuestos Internos (Internal Revenue Service, IRS) al 800.829.0433. Además, las víctimas de robo de identidad que tengan problemas para llenar sus declaraciones juradas deberán llamar a la Oficina del Defensor del Contribuyente al 877.777.4778.

- Si sus inversiones han quedado comprometidas

Informe a su intermediario o gerente de cuenta y a la Comisión Nacional del Mercado de Valores (Securities and Exchange Commission, SEC). Puede comunicarse con la SEC por Internet en www.sec.gov/complaint.shtml, por carta a la Oficina de Educación y Asistencia de Inversores (Office of Investor Education and Assistance), 450 Fifth Street, NW, Washington DC, 20549-0213 o por teléfono al 202.942.7040.

Cómo protegerse contra el robo de identidad



ROBERT M. MORGENTHAU
FISCAL





ROBERT M. MORGENTHAU
FISCAL

Queridos Amigos:

El robo de identidad es el delito de más rápido crecimiento del país. Los ladrones de identidad roban datos personales y los utilizan para obtener acceso a los recursos financieros de la víctima. La Unidad de Robo de Identidad de nuestra Oficina se concentra en todos los aspectos de este delito, incluidas las sofisticadas organizaciones delictivas que roban identidades. Este folleto le dará algunas sugerencias acerca de cómo protegerse usted y a su familia para no convertirse en víctimas. También proporciona información acerca de lo que debería hacer si es víctima del robo de identidad. Puede llamar en cualquier momento al 212.335.9600 nuestra Línea Directa de Robo de Identidad para obtener más ayuda.

Atentamente,

Robert M. Morgenthau

PREGUNTAS Y RESPUESTAS

¿Qué es el robo de identidad?

El robo de identidad es un delito cada vez más común, mediante el cual un delincuente obtiene sus datos personales, tales como su número de Seguro Social o su fecha de nacimiento, y luego los utiliza fraudulentamente para su propio beneficio. Los delitos de robo de identidad comprenden desde la utilización de una tarjeta de crédito robada para una sola compra, hasta la apertura de muchas cuentas a nombre de una víctima. Un delincuente hasta puede asumir la identidad de otra persona, en la mayoría de los casos para obtener una ganancia financiera, pero a veces para escapar del cumplimiento de la ley o comenzar una nueva vida.

¿Cómo obtienen sus datos los delincuentes?

Pueden robar su correspondencia o su billetera, revisar la basura, penetrar en las computadoras, utilizar el correo electrónico o trucos telefónicos, u obtener la ayuda de empleados de empresas deshonestos que tengan acceso legítimo a sus datos personales. Con relativamente poca información, y aún sin utilizar tecnología avanzada, delincuentes inexpertos pueden comenzar a abrir cuentas a su nombre y acumular cargos considerables.

¿Cómo puedo reducir el riesgo de convertirme en víctima del robo de identidad?

Si bien nunca puede protegerse totalmente del robo de identidad, existen medidas que puede tomar para reducir considerablemente el riesgo de ser víctima. En caso de que usted haya sido víctima de robo de identidad, existen varios modos de minimizar el daño.

¡DESTRUYA! ¡DESTRUYA! ¡DESTRUYA!

Antes de tirar documentos a la basura, destrúyalos completamente, en especial los que contengan información identificatoria. Corte en pedazos las tarjetas de crédito vencidas antes de tirarlas. Los documentos desechados intactos continúan siendo una importante fuente de datos personales utilizada por los delincuentes.

Nunca proporcione datos personales a ninguna persona o empresa que inicie contacto con Ud

Proporcione información únicamente a personas o empresas con las cuales usted se ha puesto en contacto directamente. Tenga cuidado con los correos electrónicos y las llamadas telefónicas en los que le soliciten datos personales, aunque dicha solicitud provenga de una persona o compañía que usted conoce.

Confirme la necesidad de proporcionar información personal

Si una persona o empresa le solicita información personal para abrir una cuenta o completar una operación, confirme que dicha información sea necesaria. Cuantos menos lugares tengan sus datos, será menos probable que los ladrones de identidad tengan acceso a sus datos.

Proteja su número de Seguro Social

El número de Seguro Social es probablemente la información más deseable para los delincuentes dado que permite el acceso a muchos aspectos de la vida de una persona. Nunca dé su número de Seguro Social si no está 100% seguro de que la información irá a una organización legítima y acreditada. Cuando sea posible, pida que se utilicen otros tipos de identificación. No lleve su tarjeta de Seguro Social ni nada que lo contenga ni en su billetera ni en su cartera. No imprima su número de Seguro Social en sus cheques personales.

No utilice claves ni números de identificación personal que sean obvios

No debe utilizar números de identificación personal (PIN, por sus siglas en inglés) tales como su fecha de nacimiento, los últimos cuatro dígitos de su número de Seguro Social o el nombre de soltera de su madre para acceder a sus cuentas bancarias u otra información personal.

Mantenga su información personal en un lugar seguro

No deje información personal (facturas, pasaportes o tarjetas de Seguro Social, por ejemplo) en lugares obvios en su hogar o lugar de trabajo. En caso de un asalto, no querrá que los ladrones encuentren fácilmente sus registros privados.

Proteja su correspondencia

Deposite toda la correspondencia que envíe en un buzón seguro del Servicio Postal de los Estados Unidos. Retire la correspondencia que reciba lo más pronto posible después de su llegada. Si sale de la ciudad, solicite que retengan su correspondencia en la oficina de correos o pídale a un vecino que la retire por usted.

Cancele cualquier tarjeta de crédito no utilizada

Tener más tarjetas de crédito de las que necesita aumenta su exposición al robo de identidad. También es menos probable que revise regularmente los estados de cuenta de las tarjetas de crédito no utilizadas y como consecuencia es posible que no detecte las operaciones sospechosas.

Notifique cualquier cambio de domicilio al banco

Si cambia su domicilio, asegúrese de informar a los bancos o empresas de tarjetas de crédito en las que tiene cuentas.

Cerciórese de cuándo recibe sus facturas

Preste atención respecto de cuándo recibe típicamente sus facturas. Si comienza a notar una demora en la recepción de sus facturas, o que no llegan, comuníquese con los acreedores de inmediato. Las facturas faltantes pueden ser un indicio de robo de identidad.

Solicite sus informes crediticios

Por lo menos una vez por año solicite informes crediticios a las tres sociedades de información crediticia (ver más adelante) y busque cualquier movimiento que no concuerde con sus registros. A partir del 1° de septiembre de 2005, todos los consumidores en los Estados Unidos tendrán derecho a recibir un informe crediticio sin cargo por año. Para recibir su informe sin cargo, no puede dirigirse a las tres sociedades de información crediticia individualmente; debe visitar el sitio central de Internet de las tres sociedades (www.annualcreditreport.com) o llamar al 877.322.8228. Se le dará la opción de recibir el informe de cualquiera de las tres sociedades nacionales de información crediticia.

Correo electrónico

No responda a solicitudes de extraños por correo electrónico.

Descarga de archivos

Nunca descargue archivos sospechosos ni haga clic en un hipervínculo con un sitio que no conoce.

Información confidencial en Internet

No envíe ninguna información confidencial por Internet a menos que el sitio sea seguro y que el destinatario sea una persona u organización en la que tiene total confianza.

Sitios de Internet no seguros

Evite los sitios Web no seguros. Puede determinar que un sitio es seguro por el icono del “candado” que aparece en la barra de estado al pie de su buscador de Internet.

Información financiera en su computadora

Evite guardar información financiera en su computadora, especialmente si tiene un laptop. Si mantiene registros financieros en su computadora, proteja esta información al menos con una clave. No use la función de auto-ingreso que le permite el acceso a cuentas sin escribir la clave.

Protección antivirus

Actualice su software de protección antivirus regularmente.

Firewall

Asegúrese de tener instalado un programa de firewall, especialmente si utiliza una conexión a Internet de alta velocidad.

Computadoras desechadas

Antes de tirar una computadora, reformatee todo el disco rígido. Esto hace que sea difícil para cualquiera acceder a sus archivos en el futuro.

Cierre las cuentas comprometidas

Cierre cualquier cuenta que haya quedado comprometida o que haya sido abierta fraudulentamente a su nombre.

Comuníquese con cada una de las tres principales sociedades de información crediticia

Póngase en contacto con las tres Sociedades de Información Crediticia para solicitar una copia de su informe crediticio y colocar una alerta de fraude en su cuenta.

• Sociedades de información crediticia

Las sociedades de información crediticia son empresas que proporcionan informes de crédito sobre posibles prestatarios a las entidades de préstamo. Las entidades de préstamos tales como las empresas de tarjetas de crédito y los bancos, típicamente consultan a las sociedades de información crediticia antes de decidir el otorgamiento de un crédito.

• Informes crediticios

Los informes crediticios incluyen el nombre del posible prestatario, su domicilio, su número de Seguro Social y su fecha de nacimiento; las cuentas con las que opera, incluidos los saldos y límites de crédito; la puntualidad en el pago; las cantidades cobradas; cualquier juicio, fallo o gravamen por impuestos no pagados y otra información adicional. Revisar una copia de su propio informe de crédito le permitirá verificar que no exista ninguna cuenta no autorizada a su nombre.

• Alerta de fraude

Al colocar una alerta de fraude en su cuenta con las sociedades de información crediticia, usted solicita que la sociedad de información crediticia le avise por teléfono (se sugiere utilizar un teléfono celular por razones prácticas) cuando una entidad de préstamo pregunte acerca de abrir una nueva cuenta a su nombre. De este modo, puede averiguar si alguna persona que no sea usted ha intentado abrir cuentas a su nombre. De allí en más, puede tomar medidas y limitar el daño de sus antecedentes crediticios.

Cómo comunicarse con las Sociedades de Información Crediticia

• Equifax

www.equifax.com

800.685.1111 (para solicitar su informe crediticio)

800.525.6285 (para informar un fraude)

• Experian

www.experian.com

888.397.3742 (para solicitar su informe crediticio o para informar un fraude)

• TransUnion

www.transunion.com

800.888.4213 (para solicitar su informe crediticio)

800.680.7289 (para informar un fraude)

Para recibir su informe crediticio anual sin cargo, debe utilizar otro sitio Web y número de teléfono: www.annualcreditreport.com u 877.322.8228.

Llame a la Policía

La policía no sólo puede ser útil para atrapar al delincuente, sino que también prepara una denuncia policial que usted necesitará para probar a sus acreedores que ha sido víctima de un fraude de identidad.

Comuníquese con la Línea Directa de la Unidad de Robo de Identidad de la Fiscalía del Condado de Nueva York

al 212.335.9600. El personal de la unidad está compuesto por fiscales adjuntos con experiencia en el procesamiento por delitos de robo de identidad

Comuníquese con la Línea Directa de Robo de Identidad de la Comisión Federal de Comercio (Federal Trade Commission)

Para presentar una denuncia a la FTC, llame al 877.438.4338. Para obtener más información sobre qué hacer si ha sido víctima de un robo de identidad, visite el sitio Web de la FTC: www.consumer.gov/idtheft/.

Notifique a cualquier entidad en la que tiene una cuenta

Si no está seguro de la medida en que se ha utilizado fraudulentamente su identidad, debe notificar a todas las empresas de tarjetas de crédito, bancos, empresas de telefonía celular u otras empresas en las que tenga una cuenta. Para cerciorarse de que un delincuente no esté explotando su condición profesional, se sugiere también que se comunique con todas las organizaciones profesionales de las que es miembro.

Contactos para tipos específicos de robo

• **Si le han robado su Licencia de Conducir o su Identificación de No Conductor**

Si el delincuente ha obtenido una licencia de conducir o una identificación de no conductor a su nombre, comuníquese con la sucursal local del Departamento de Automotores.

• **Si se está utilizando fraudulentamente su número de Seguro Social**

Puede dirigirse a la Oficina del Inspector General de la Administración del Seguro Social por teléfono al: 800.269.0271; por fax: 410.597.0118; por correo: SSA Fraud Hotline, P.O. Box 17768, Baltimore, MD 21235; o por correo electrónico: oig.hotline@ssa.gov. También puede llamar a la Administración del Seguro Social al 800.772.1213 para verificar la exactitud de las ganancias informadas para su Número de Seguro Social, solicitar una copia de su Declaración de Seguro Social, u obtener una Tarjeta de Seguro Social de reemplazo, si ha extraviado la suya o se la han robado.

• **Si le han robado su correspondencia o si un delincuente ha cambiado fraudulentamente su domicilio**

Puede dirigirse al Servicio de Inspección Postal de los Estados Unidos (U.S. Postal Inspection Service, USPIS) e informar sobre el robo al inspector postal local. Puede localizar la oficina de distrito de la USPIS más cercana llamando a su oficina postal local o verificando la lista en www.usps.gov/websites/depart/inspect.

• **Si le han robado su pasaporte o lo ha extraviado**

Si le han robado su pasaporte, lo ha extraviado o si alguien lo está utilizando fraudulentamente, diríjase al Departamento de Estado de los Estados Unidos (USDS) en www.travel.state.gov/passport_services.html o llame a una oficina local del USDS. La lista de oficinas locales se publica en las Páginas Azules de su guía telefónica.