Todo sobre el ROBO DE IDENTIDAD

Comisión Federal de Comercio
Junio 2005

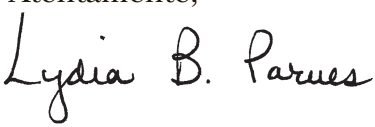
Estimado Consumidor:

La Comisión Federal de Comercio (*Federal Trade Commission*, FTC) ha publicado este folleto para acrecentar el nivel de conocimiento sobre el robo de identidad. Lo alentamos a compartir esta publicación con su familia, amigos, colegas y vecinos.

Si alguien ha utilizado su nombre u otra información personal para cometer fraude, por favor visite en Internet **ftc.gov/robodeidentidad** para enterarse cómo proceder y cuál es la manera de presentar una queja sobre robo de identidad. En el sitio Web de la FTC también encontrará enlaces útiles que contienen información de otras agencias federales y estatales y de organizaciones de consumidores. La información contenida en su queja pasará a formar parte de una base de datos segura utilizada por funcionarios a cargo del cumplimiento de la ley de todo el país para colaborar en la tarea de detener las prácticas de los ladrones de identidad.

Si no tiene acceso al Internet, llame a la línea gratuita de asistencia de la FTC para casos de robo de identidad 1-877-ID-THEFT.

Atentamente,



Lydia B. Parnes, Directora
Bureau of Consumer Protection
Federal Trade Commission

CONTENIDO

INTRODUCCIÓN

En el transcurso de un día agitado, usted puede hacer un cheque en el almacén, comprar boletos para un partido de fútbol con su tarjeta de crédito, alquilar un auto, enviar por correo su declaración de impuestos, cambiar de proveedor de servicio de teléfono celular o solicitar una nueva tarjeta de crédito. Cada vez que realiza una de estas transacciones, usted revela partes de su información personal, como por ejemplo los números de su cuenta bancaria o de tarjeta de crédito; sus ingresos; su número de Seguro Social; o su nombre, domicilio y números telefónicos — cada unos de estos datos es una mina de oro para un ladrón de identidad. Una vez que un ladrón obtiene esa información, puede utilizarla para robar o cometer fraude sin su conocimiento.

El robo de identidad es un delito serio. Las personas cuyas identidades han sido robadas pueden perder tiempo y dinero reparando los perjuicios que los ladrones han causado a sus registros de crédito y a su buen nombre. Las victimas pueden perder oportunidades de empleo, sus solicitudes de préstamo para estudios, vivienda o automóviles pueden ser rechazadas y hasta pueden ser arrestados por delitos que no cometieron.

¿Puede usted prevenir convertirse en víctima del robo de identidad? Al igual de lo que sucede con otros delitos, usted no puede controlarlo completamente. Pero, según la FTC, la agencia nacional de protección del consumidor, usted puede minimizar su riesgo manejando su información personal con más cautela.

CÓMO SE PRODUCE EL ROBO DE IDENTIDAD

Los "especialistas" en robo de identidad pueden valerse de una variedad de métodos para acceder a su información personal. Por ejemplo, pueden obtener su información consiguiéndola en negocios u otras instituciones mientras que se encuentran en el trabajo; sobornando a un empleado que tiene acceso a los registros, "pirateando" esos registros y engañando a los empleados para obtener información. O:

- Pueden robarle su billetera, cartera o bolso.
- Pueden robar su información personal a través de su e-mail o teléfono haciéndose pasar por representantes de compañías con la excusa de que existe un problema con su cuenta. Esta práctica es conocida en inglés con el nombre de *phishing* cuando se realiza en línea o "llamada pretextada" (*pretexting*) cuando se hace por teléfono.
- Pueden robar los números de sus tarjetas de crédito o débito capturando la información mediante un dispositivo de almacenamiento de datos en una práctica conocida en inglés como *skimming*. Pueden pasar su tarjeta para hacer una compra real o conectar un dispositivo a una máquina ATM en la cual usted inserte o pase su tarjeta.
- Pueden obtener sus informes crediticios aprovechándose indebidamente del acceso autorizado que sus empleadores tienen a estos registros, o pueden hacerse pasar por un propietario de vivienda, empleador o alguna otra persona que pudiera tener un

derecho legal para acceder a su informe crediticio.

- Pueden revolver la basura de su casa, los residuos de comercios y negocios o los basureros ubicados en la vía pública mediante una práctica conocida como "búsqueda de basureros" (*dumpster diving*).
- Pueden robar la información personal que encuentren en su casa.
- Pueden robar su correspondencia, en la que podrían encontrar resúmenes de cuentas bancarias y de tarjetas de crédito, ofrecimientos de tarjetas de crédito, cheques nuevos e información impositiva.
- Pueden completar un "formulario de cambio de domicilio" para derivar su correspondencia hacia otro lugar.

Una vez que los ladrones de identidad consiguen su información personal, pueden utilizarla para cometer fraude o robo. Por ejemplo:

- Pueden llamar al emisor de su tarjeta de crédito para solicitar el cambio de domicilio de su cuenta. El impostor, entonces, efectúa gastos con su tarjeta. Dado que sus facturas son enviadas a un domicilio diferente, puede que pase algún tiempo antes de que usted se dé cuenta de que existe un problema.
- Pueden abrir nuevas cuentas de tarjeta de crédito a nombre de otra persona. Cuando

los ladrones de identidad usan las tarjetas de crédito y no pagan las facturas, las cuentas impagas son reportadas al informe crediticio del consumidor afectado.

- Pueden establecer servicios de teléfono o celular a nombre de otra persona.
- Pueden abrir una cuenta bancaria a nombre de otra persona y emitir cheques sin fondos sobre esa cuenta.
- Pueden falsificar cheques o tarjetas de crédito o débito, o autorizar transferencias electrónicas a nombre de otra persona y vaciar la cuenta bancaria de la víctima.
- Pueden declararse en bancarrota bajo otro nombre — el de la víctima — para evitar el pago de las deudas en que hubieran incurrido o para evitar el desalojo.
- Pueden comprar un automóvil o sacar un préstamo para automóviles a nombre del consumidor afectado.
- Pueden obtener documentos de identidad, como por ejemplo una licencia para conducir emitida con la fotografía del impostor, pero a nombre de otra persona.
- Pueden obtener un empleo o presentar declaraciones de impuestos fraudulentas a nombre del consumidor afectado.
- Durante un arresto pueden identificarse ante la policía con otro nombre. En caso de que no se presenten ante la corte en la fecha establecida, se expedirá una orden de arresto a nombre de la víctima del robo de identidad.

¿CÓMO PUEDE SABER SI ES VÍCTIMA DEL ROBO DE IDENTIDAD?

Si un ladrón de identidad abre nuevas cuentas de crédito a su nombre, es muy probable que estas cuentas aparezcan en su informe crediticio. Usted puede averiguarlo solicitando una copia de su informe crediticio a cada una de las compañías de informes de los consumidores del país. En caso de que hubiera perdido o le hubieran robado algún tipo de información personal, sería bueno que verifique todos sus informes más frecuentemente durante el primer año.

Examine los saldos de sus cuentas financieras. Contrólelos para verificar si se le han imputado cargos o retiros inexplicables. Otros indicadores del robo de identidad pueden ser:

- No recibir facturas u otra correspondencia, lo que podría indicar que un ladrón de identidad hizo un cambio de domicilio.
- Recibir tarjetas de crédito que usted no solicitó.
- Denegación de crédito sin razón aparente.
- Recibir llamados de cobradores de deuda o compañías sobre mercaderías o servicios que usted no compró.

CÓMO OBTENER SU INFORME CREDITICIO

INFORMES CREDITICIOS ANUALES GRATUITOS
Una enmienda recientemente introducida a la ley federal llamada *Fair Credit Reporting Act* (FCRA) requiere que, a su pedido, cada una de las compañías de informes de los consumidores del país le provea una copia gratuita de su informe de crédito cada 12 meses.

Los informes crediticios gratuitos anuales comenzaron a suministrarse durante un período escalonado de nueve meses que se extenderá desde los estados de la región oeste hacia los de la región este del país. A partir del 1º de septiembre de 2005 todos los estadounidenses podrán acceder a sus informes crediticios anuales gratuitamente independientemente de la región en la que residan.

Para solicitar su informe de crédito anual gratuito a una o a todas las compañías de informes de los consumidores del país visite en Internet **www.annualcreditreport.com**, llame al 1-877-322-8228 o complete el formulario llamado *Annual Credit Report Request Form* y envíelo por correo a: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Puede imprimir el formulario descargándolo desde **ftc.gov/credito**. La solicitud debe ser hecha en inglés. No tome contacto individualmente con cada una de las tres compañías de informes de los consumidores del país. Estas compañías solamente suministran informes de crédito gratuitos a través de **www.annualcreditreport.com**, 1-877-322-8228 y Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

OTROS DERECHOS DE LOS CONSUMIDORES PARA OBTENER INFORMES CREDITICIOS GRATUITOS

Bajo lo dispuesto por ley federal, usted tiene derecho a recibir un informe gratuito si una compañía toma una acción adversa en su contra, como por ejemplo la denegación de su solicitud de crédito, seguro o empleo y usted solicita su informe dentro de un plazo de 60 días contado a partir de la fecha de recepción de la notificación de la acción adversa. La notificación de la acción adversa le proporcionará el nombre, domicilio y número de teléfono de la compañía de informes de los consumidores que suministró la información sobre usted. Usted también tiene derecho a obtener un informe gratuito en caso de que se encuentre desempleado y tenga planes de buscar empleo dentro de los 60 días; si usted recibe asistencia pública; o si su informe es inexacto debido a un fraude. De lo contrario, una compañía de informes de los consumidores puede cobrarle hasta $9.50 por cada informe de crédito adicional solicitado.

PARA COMPRAR UNA COPIA DE SU INFORME, TOME CONTACTO CON:

- **Equifax:** 1-800-685-1111; www.equifax.com
- **Experian:** 1-888-EXPERIAN (1-888-397-3742); www.experian.com
- **TransUnion:** 1-800-916-8800; www.transunion.com

Bajo lo establecido por la ley estatal, los consumidores de Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey y Vermont tienen derecho a obtener informes de crédito gratuitamente.

Puede solicitar que en sus informes de crédito aparezcan solamente los últimos cuatro dígitos de su número de Seguro Social.

CÓMO MANEJAR SU INFORMACIÓN PERSONAL

¿Cómo puede actuar un consumidor responsable para minimizar el riesgo y el daño potencial del robo de identidad? Cuando se trate de su información personal, sea cauto y prudente.

HÁGALO YA

Ponga contraseñas en sus tarjetas de crédito, cuentas bancarias y telefónicas. Evite utilizar como contraseña información que sea de fácil disponibilidad como por ejemplo su apellido materno, su fecha de nacimiento, los últimos cuatro dígitos de su número de Seguro Social, su número de teléfono o una serie de números consecutivos. Cuando presente una solicitud para una cuenta nueva, posiblemente encuentre que algunas compañías aún incluyen una línea para que escriba su apellido materno. En su lugar, pida que le dejen colocar una contraseña.

Resguarde su información personal dentro de su casa, especialmente si comparte la vivienda con otras personas o si recibe asistencia de empleados o servicios externos o si se están realizando trabajos o reparaciones en su vivienda.

Consulte los procedimientos de seguridad implementados para resguardar la información personal en su lugar de trabajo, consultorio de su médico u otras instituciones que registran su información de identificación personal. Averigüe quién tiene acceso a sus datos personales y verifique que los registros estén manejados

de manera segura. También pregunte cuáles son los procedimientos de eliminación de los registros que contienen información personal. Averigüe si su información será compartida con alguien más, y si así fuera pregunte si pueden mantener sus datos en forma confidencial.

DILIGENCIAS COTIDIANAS

No dé su información personal por teléfono, por correo o a través del Internet a no ser que sea usted quien haya iniciado el contacto o sepa con quien está tratando. Los ladrones de identidad actúan astutamente y para lograr que los consumidores revelen su información personal — número de Seguro Social, apellido materno, números de cuentas y demás datos — fingen ser empleados bancarios, prestadores de servicios de Internet (ISP) y hasta representantes de agencias gubernamentales. Antes de compartir cualquier información personal confirme que está tratando con una organización legítima. Para verificar el sitio Web de una organización escriba su dirección de Internet en la línea destinada al domicilio Web en vez de usar la función de cortar y pegar. Muchas compañías ponen en línea alertas de estafas o fraudes cuando sus nombres son invocados indebidamente, también puede llamar al servicio al cliente comunicándose con el número que figura en su resumen de cuenta o en la guía telefónica.

Maneje su correspondencia y su basura cuidadosamente. Deposite el correo que envía en buzones ubicados en oficinas postales o en la oficina postal local en vez de hacerlo en buzones no custodiados. Cuando pase el cartero, retire el correo de su buzón inmediatamente. Si tiene planes de ausentarse de su casa por un tiempo y no pudiera recoger su correo, notifique al Servicio Postal de los Estados Unidos, 1-800-275-8777, y solicite el servicio de retención de correo. El servicio postal retendrá su correo en sus oficinas hasta que, a su regreso, usted lo recoja o reanude el servicio.

Antes de desechar papelería que contenga información personal destruya todos los recibos, copias de solicitudes de tarjetas de crédito, formularios de seguros, informes médicos, cheques y resúmenes de cuentas bancarias, tarjetas de crédito o cuentas abiertas por 30 días (*charge card*) vencidas y ofertas de crédito personalizadas que recibe a través del correo, de esta manera frustrará las intenciones de un ladrón de identidad que pudiera buscar información personal revolviendo la basura o cestos de desechos reciclables. Para optar por no recibir más ofrecimientos de crédito por correo, llame a: 1-888-5-OPTOUT (1-888-567-8688). Las tres compañías de informes de los consumidores de todo el país utilizan el mismo número telefónico gratuito, mediante este número se les permite a los consumidores optar por no recibir ofrecimientos de crédito basados en sus listas. **Nota:** Se le solicitará que suministre su número de Seguro Social ya que las compañías de informes de los consumidores lo necesitarán para identificar su registro.

No lleve consigo su tarjeta de Seguro Social, guárdela en un lugar seguro.

Dé su número de Seguro Social únicamente cuando sea absolutamente indispensable y cuando sea posible, utilice otro tipo de identificación. Si en el estado en el que reside se utiliza el mismo número de Seguro Social en su licencia para conducir, solicite que lo sustituyan por otro. Haga lo mismo si su compañía de seguro de salud lo utiliza como número de póliza.

Cuando salga, lleve consigo únicamente la información de identificación y la cantidad de tarjetas de crédito y débito que realmente necesita. Si pierde o le roban su cartera o billetera, repórtelo inmediatamente a los emisores de sus tarjetas y a la policía local.

Sea cauto cuando responda a las promociones. Los ladrones de identidad pueden crear ofertas u ofrecimientos promocionales falsos para lograr que usted les dé su información personal.

Conserve su billetera, cartera o bolso en un lugar seguro en su trabajo; haga lo mismo con las copias de los formularios administrativos que contengan información personal delicada.

Cuando pida chequeras nuevas, en vez de que se las envíen por correo a su casa retírelas directamente del banco.

CONSIDERE LA SEGURIDAD DE SU COMPUTADORA

Su computadora puede ser una mina de oro de información personal para un ladrón de identidad. A continuación se enumeran algunas recomen-

daciones para ayudarlo a mantener segura su computadora y la información personal almacenada en la misma.

- Actualice regularmente sus programas antivirus, instale las reparaciones de seguridad de su sistema operativo y demás programas para protegerse contra las intrusiones e infecciones que podrían comprometer los archivos de su computadora o sus contraseñas. Lo ideal es establecer una actualización semanal del programa de protección antivirus. El sistema operativo Windows XP también puede instalarse de manera tal que verifique e instale automáticamente las actualizaciones de este tipo.
- No abra archivos enviados por extraños, no presione sobre vínculos o enlaces ni descargue programas enviados por personas o compañías desconocidas. Sea cuidadoso al utilizar la opción de archivos compartidos. La apertura de un archivo puede exponer su computadora a un programa o infección con un virus cibernético conocido como "programa espía" (*spyware*) el cual tiene la capacidad de capturar sus contraseñas o cualquier otra información a medida que usted la escribe en el teclado.
- Use un programa *firewall*, especialmente si utiliza un acceso de alta velocidad o banda ancha para conectarse al Internet — como cable, DSL o T-1 — el cual mantienen conectada su computadora al Internet las 24 horas del día. El programa *firewall* impedirá que los visitantes indeseados accedan a su computadora. Sin la instalación de este programa, los *hackers* o piratas informáticos pueden acceder a su computadora y a la información personal

almacenada en la misma o utilizar los datos para cometer otros delitos.

- Si necesita proveer su información personal o financiera a través del sitio Web de una organización, busque los indicadores de seguridad del sitio, como por ejemplo el símbolo del candado en la barra de estado del navegador o fíjese si la dirección del sitio Web comienza con "https:" (la letra "s" significa seguro). Lamentablemente, ningún indicador es cien por ciento confiable, hay algunos sitios fraudulentos que han falsificado los íconos de seguridad.

- Trate de no almacenar información financiera en su computadora portátil a menos que sea absolutamente necesario. Si guarda este tipo de información, utilice una contraseña sólida — una combinación de letras (mayúsculas y minúsculas), números y símbolos. Un buen método para crear una contraseña sólida es pensar en una frase fácil de memorizar y utilizar la primera letra de cada palabra como contraseña, convirtiendo algunas de las letras en números. Por ejemplo, "Me pareció ver un lindo gatito", podría convertirse en MPV1L6. No emplee la característica de conexión automática ya que ésta guarda su nombre de usuario y contraseña y no requiere que usted los ingrese cada vez que se conecta o que accede a un sitio en la red. Desconéctese siempre cuando termine. De esta manera, si le roban su computadora portátil será más difícil que el ladrón pueda acceder a su información personal.

- Antes de desechar una computadora, elimine toda la información personal almacenada en la misma. Eliminar los archivos a través de los comandos del teclado o del ratón o reformatear el disco duro puede ser insuficiente porque dichos archivos probablemente permanezcan en el disco duro de su computadora y por lo tanto pueden ser fácilmente recuperados. Utilice un programa de borrado o eliminación de archivos (*wipe utility program*) para sobrescribir completamente el disco duro.
- Busque las políticas de privacidad de los sitios Web y léalas. Las políticas de privacidad deben describir la manera en que los sitios Web mantienen la exactitud, acceso, seguridad y control de la información personal recogida, como así también cómo será utilizada y si será provista a terceros. Si no encuentra la política de privacidad — o no la entiende — mejor considere visitar otros sitios Web.

COMENTARIO SOBRE LOS NÚMEROS DE SEGURO SOCIAL

Su empleador e instituciones financieras necesitan su número de Seguro Social para fines de pagos de salarios y declaraciones impositivas. Otros negocios pueden solicitarle su número de Seguro Social para hacer una verificación de crédito, por ejemplo cuando solicita un préstamo, alquila un apartamento o se registra para un servicio público. Sin embargo, en algunas oportunidades solamente le solicitan ese número para sus registros. Si alguien le pide su número de Seguro Social hágale las siguientes preguntas:

- ¿Por qué necesita mi número de Seguro Social?
- ¿Cómo será utilizado mi número de Seguro Social?
- ¿Cómo será protegido mi número de Seguro Social?
- ¿Qué sucederá si no le doy mi número de Seguro Social?

En algunas situaciones, si usted no suministra su número de Seguro Social algunos comercios pueden no proveerle la mercadería, servicio o beneficio solicitado. Las respuestas a estas preguntas lo ayudarán a decidir si usted desea darle esta información al negocio que se la pida. Recuerde que la decisión es suya.

ALERTAS DE FRAUDE PARA PERSONAL MILITAR EN SERVICIO ACTIVO

Si usted es miembro de las fuerzas armadas y se encuentra lejos de su repartición habitual, puede colocar una alerta de servicio activo en sus informes crediticios comunicándose con cualquiera de las tres compañías principales de informes de los consumidores. Este tipo de alertas puede ser útil para minimizar el riesgo de robo de identidad durante el tiempo que usted se encuentre desplazado en cumplimiento de funciones. Para colocar una alerta en su informe crediticio o para quitarla, tendrá que verificar su identidad suministrando su número de Seguro Social, nombre, domicilio y demás información personal solicitada por la compañía de informes del consumidor. Para registrar o quitar una alerta usted puede valerse de un representante personal.

Las alertas por servicio activo permanecen en efecto en su informe crediticio durante un año. En caso de que su misión se extienda por más tiempo, usted puede colocar otra alerta en su informe crediticio.

Cuando un negocio ve la alerta registrada en su informe crediticio, debe verificar su identidad antes de otorgarle crédito. Como parte de este proceso de verificación, es posible que el negocio intente contactarlo directamente, este procedimiento puede causar cierta demora si usted está tratando de obtener crédito. Para prevenir posibles

demoras, asegúrese de mantener actualizada su información de contacto.

Cuando usted coloca una alerta por servicio activo en su informe crediticio, también se quitará su nombre de las listas de comercialización de las compañías de informes de los consumidores para ofrecimientos de tarjetas preevaluadas durante dos años, a menos que usted solicite que lo vuelvan a incluir en la lista antes de que expire ese plazo.

QUÉ HACER SI SU INFORMACIÓN HA SIDO ROBADA O PERDIDA

En caso de que hubiera perdido o le hubieran robado documentos u otros papeles que contengan información personal, usted puede minimizar la posibilidad de convertirse en víctima del robo de identidad actuando rápidamente.

- **Cuentas con instituciones financieras:** Cierre inmediatamente las cuentas bancarias o de tarjeta de crédito. Cuando abra cuentas nuevas, póngales contraseñas. Evite utilizar como contraseña su apellido materno, su fecha de nacimiento, los cuatro últimos dígitos de su número de Seguro Social, su número de teléfono o una serie de números consecutivos.

- **Número de Seguro Social:** Llame a la línea gratuita destinada a denuncias de fraudes de cada una de las tres compañías de informes de los consumidores del país y coloque una **alerta inicial de fraude** en sus informes crediticios (véase página 23). Una alerta de este tipo puede ser útil para impedir que alguien abra nuevas cuentas de crédito a su nombre.

- **Licencias para conducir/otros documentos de identidad emitidos por el gobierno:** Comuníquese con la agencia emisora de la licencia u otro documento de identidad.

Siga los procedimientos de la agencia para cancelar el documento y obtener uno de reemplazo. Pídale a la agencia que señale el incidente en su registro para que nadie más pueda tramitar una licencia ni cualquier otro documento de identidad a su nombre ante esa agencia.

Una vez que haya tomado estas precauciones, manténgase alerta ante la aparición de signos que puedan indicar que su información está siendo utilizada indebidamente y que su identidad ha sido robada.

Si su información ha sido utilizada indebidamente, efectúe una denuncia del robo ante la policía y también presente una queja ante la FTC. Si se hubiera cometido algún otro delito — por ejemplo, si su cartera o billetera hubiera sido robada, o si alguien hubiera ingresado a su casa o violentado su auto — repórtelo a la policía inmediatamente.

VÍCTIMAS DEL ROBO DE IDENTIDAD: PASOS QUE SE DEBEN TOMAR INMEDIATAMENTE

Si usted es una víctima del robo de identidad, siga los siguientes cuatro pasos tan pronto como le sea posible y conserve un registro con todos los detalles de sus conversaciones y copias de su correspondencia sobre el tema. También puede conseguir una copia de la publicación de la FTC titulada *Tome Control: Defiéndase Contra el Robo de Identidad*, una guía completa que le brindará información sobre temas tales como qué hacer, cuáles son sus derechos legales, cómo manejar los problemas específicos que puede enfrentar en el proceso de reinstaurar su buen nombre y cuáles son los indicadores a los que deberá estar atento en el futuro. Esta guía también incluye la Declaración Jurada de Robo de Identidad que es un documento que le será de utilidad para reportar información a varias compañías. Para más información, consulte en Internet **ftc.gov/robodeidentidad**.

1. **Coloque una alerta de fraude en sus informes crediticios y revíselos.**
   Las alertas de fraude pueden ayudar a prevenir que un ladrón de identidad continúe abriendo más cuentas a su nombre. Comuníquese con la línea gratuita destinada a fraudes de alguna de las tres compañías de informes de los consumidores que se listan a continuación para colocar una alerta de fraude en su informe crediticio. Para hacerlo, solamente tiene que llamar a una de las tres compañías.

La compañía a la que usted llame está obligada a comunicarse con las otras dos, las cuales a su vez también colocarán una alerta en los informes crediticios que mantengan a su nombre.

- **Equifax:** 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
- **Experian:** 1-888-EXPERIAN (1-888-397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013
- **TransUnion:** 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Cuando usted coloque la alerta de fraude en su registro, tiene derecho a solicitar copias de sus informes crediticios gratuitamente, y en caso de que lo solicite, en sus informes solamente aparecerán los cuatro últimos dígitos de su número de Seguro Social. Cuando reciba sus informes crediticios, revíselos cuidadosamente. Busque averiguaciones iniciadas por compañías con las que usted no mantiene una relación comercial, cuentas que usted no abrió y deudas inexplicables imputadas a su cuenta. Verifique que los datos tales como su número de Seguro Social, domicilio(s), nombre o iniciales y empleadores estén registrados correctamente. Si usted encuentra información fraudulenta o incorrecta, contacte a las compañías de informes de los consumidores y pida que la quiten de su registro. Continúe controlando sus informes crediticios periódicamente, especialmente durante el primer año después

de la fecha en que descubra el robo de identidad para asegurarse de que no se produjo nueva actividad fraudulenta.

ALERTAS DE FRAUDE

- **Una alerta inicial permanece en su informe crediticio por lo menos durante 90 días.** Usted puede solicitar que se coloque una alerta inicial en su informe crediticio si sospecha que ha sido o podría convertirse en una víctima del robo de identidad. Es apropiado solicitar una alerta inicial cuando le han robado la cartera o si lo han atrapado con una estafa de tipo *phishing*. Cuando usted coloca una alerta inicial en su informe crediticio tiene derecho a recibir gratuitamente una copia de su informe de parte de cada una de las tres compañías de informes de los consumidores de todo el país.
- **Una alerta prolongada permanece en su informe crediticio durante siete años.** Usted puede solicitar que se coloque una alerta prolongada en su informe crediticio si usted ha sido víctima del robo de identidad y le entrega a la compañía de informes de los consumidores un reporte de robo de identidad (véase página 24). Cuando usted coloca una alerta prolongada en su informe crediticio, tiene derecho a recibir gratuitamente dos copias de su informe de crédito de parte de cada una de las tres compañías de informes de los consumidores de todo el país dentro de los 12 meses.

Para solicitar que se registre cualquiera de estas alertas de fraude en su informe crediticio, o para quitarlas, se le requerirá que suministre datos que acrediten su identidad, entre los que pueden encontrarse: su número de Seguro Social, nombre,

domicilio y demás información personal solicitada por la compañía de informes de los consumidores.

Cuando un negocio ve la alerta registrada en su informe crediticio, debe verificar su identidad antes de otorgarle crédito. Como parte de este proceso de verificación, es posible que el negocio intente contactarlo directamente. Este procedimiento puede causar cierta demora si usted está tratando de obtener crédito. Para prevenir las posibles demoras, si lo desea puede incluir en su alerta un número de teléfono celular en el que se le pueda localizar fácilmente. Recuerde mantener actualizada toda su información de contacto incluida en la alerta.

REPORTE DE ROBO DE IDENTIDAD

Un reporte de robo de identidad se compone de dos partes:

La **Primera Parte** consta de una copia de la denuncia presentada ante una agencia de seguridad o de cumplimiento de la ley ya sea local, estatal o federal, como por ejemplo su departamento local de policía, la oficina de su Fiscal General estatal, el FBI, el Servicio Secreto de los EE.UU., la FTC y el Servicio de Inspección Postal de los EE.UU. No existe ninguna ley federal que obligue a una agencia federal a tomar una denuncia por robo de identidad; pero sin embargo, algunas leyes estatales requieren que los departamentos de policía tomen este tipo de denuncias. Cuando usted presente una denuncia, proporcione toda la información posible sobre el delito, incluyendo todo lo que usted sepa sobre las fechas en que se produjo el robo de identidad, las cuentas fraudulentas abiertas y el nombre del presunto ladrón.

La **Segunda Parte** de un reporte de robo de identidad depende de las normas de la compañía de informes de los consumidores y del proveedor de información (el negocio o comerciantes que le han enviado la información a la agencia de informes). Para verificar su identidad, es posible que le soliciten que suministre información o documentación adicional a la incluida en la denuncia policial. Pueden solicitarle la información adicional dentro de los 15 días después de la recepción de su denuncia policial, o en caso de que usted ya hubiera logrado que se registre una alerta de fraude prolongada en su informe crediticio, a partir de la fecha en que usted presente su solicitud ante la compañía de informes del consumidor para que se efectúe el bloqueo de la información. A partir de entonces, la compañía de informes de los consumidores y el proveedor de información cuentan con 15 días más para contactarlo y asegurarse de que su denuncia de robo de identidad contiene toda la información necesaria y tienen derecho a tomarse cinco días suplementarios para revisar cualquier información que usted les hubiera proporcionado. Por ejemplo, si usted les proveyó la información 11 días después de solicitada, ellos no están obligados a tomar una decisión final hasta tanto hayan transcurrido 16 días después de la fecha en que le solicitaron dicha información. Si usted les suministra cualquier información pasado el plazo de 15 días, pueden rechazar su reporte de robo de identidad por estar incompleto; en este caso, usted tendrá que volver a presentar su reporte con la información correcta.

2. Cierre aquellas cuentas que usted sepa o crea que han sido falsificadas o abiertas fraudulentamente.
Llame a cada compañía y hable con el personal del departamento de seguridad o fraude. Haga un seguimiento por escrito e incluya copias (NO originales) de los documentos que respalden su caso. *Es importante que la notificación a las compañías emisoras de tarjetas de crédito y a los bancos se haga por escrito.* Envíe sus cartas por correo certificado y solicite un acuse de recibo para poder documentar la fecha en que la compañía recibió su correspondencia. Mantenga un registro de su correspondencia y todos los documentos adjuntados.

Cuando abra cuentas nuevas, utilice nuevos números de identificación personal (*Personal Identification Numbers*, PINs) y contraseñas. Evite utilizar como contraseña datos que pudieran ser de fácil disponibilidad, como por ejemplo el apellido de su madre, su fecha de nacimiento, los cuatro últimos dígitos de su número de Seguro Social, su número de teléfono o una serie de números consecutivos.

En caso de que un ladrón de identidad haga cargos o débitos en sus cuentas, o en cuentas abiertas fraudulentamente, solicítele a la compañía los formularios para disputar dichas transacciones:

- Para cargos o débitos en cuentas preexistentes, solicite que le envíen los formularios de disputa de la compañía. Si la compañía no posee formularios especiales, escriba una carta para

cuestionar los cargos o débitos fraudulentos. En cualquiera de los casos, dirija su carta al domicilio de la compañía destinado a averiguaciones de facturación (*billing inquiries*), NO al domicilio al cual manda sus pagos.

- Para cuentas nuevas no autorizadas, pregunte si la compañía acepta la Declaración Jurada de Robo de Identidad. En caso de que no la acepten, solicite que le envíen los formularios de la compañía para presentar una disputa por fraude. Si la compañía ya reportó estas cuentas o deudas a su informe crediticio, dispute la información fraudulenta.

Una vez que haya resuelto su disputa de robo de identidad con la compañía, pida que le entreguen una carta en la que se establezca que la compañía ha cerrado las cuentas disputadas y que lo han relevado de las deudas fraudulentas. Esta carta es su mejor prueba en caso de que reaparezcan errores relacionados con esta cuenta en su informe crediticio o si vuelven a contactarlo por la deuda contraída fraudulentamente.

3. **Presente una denuncia en la dependencia policial local o en aquella dependencia policial del lugar en el cual se produjo el robo de identidad.**
Obtenga una copia de la denuncia policial o por lo menos el número de reporte o denuncia. Este comprobante podrá ayudarlo a lidiar con los acreedores que necesiten una prueba del delito. En caso de que la policía se mostrara reacia a tomarle su denuncia, solicite que le tomen una "Denuncia por Incidentes

Varios" (*Miscellaneous Incidents report*) o intente hacerlo en otra jurisdicción, como por ejemplo en las dependencias de su policía estatal. También puede consultar con la oficina de su Fiscal General estatal para averiguar si la ley estatal dispone que la policía tome denuncias por robo de identidad. Para conseguir la lista de los Fiscales General estatales, consulte las páginas azules de su guía telefónica o visite en Internet **www.naag.org**.

4. **Presente una queja ante la Comisión Federal de Comercio.**
   Al compartir los datos de su queja con la FTC, usted proporcionará información importante que puede ayudar a los funcionarios a cargo del cumplimiento de la ley de todo el país a perseguir a los ladrones de identidad y detener sus actividades. La FTC también puede derivar las quejas de las víctimas del robo de identidad a otras agencias gubernamentales y compañías para que tomen acciones adicionales, como también investigar a las compañías por las violaciones de las leyes a las que la Comisión da cumplimiento.

   Usted puede presentar una queja en Internet visitando **ftc.gov/robodeidentidad**. Si no tiene acceso al Internet, llame a la línea gratuita de asistencia para víctimas de robo de identidad: 1-877-ID-THEFT (1-877-438-4338); TDD: 202-326-2502; o escriba a: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

En caso de que obtuviera información adicional o se le presentaran nuevos problemas, llame nuevamente a la línea gratuita de asistencia para actualizar su información.

PARA MÁS INFORMACIÓN

La FTC dispone de una serie de publicaciones que tratan sobre la importancia de la privacidad de la información personal. Para solicitar copias gratuitas de los folletos, consulte en Internet **ftc.gov/ordenar** o llame al 1-877-FTC-HELP (1-877-382-4357).

Cómo Evitar el Fraude con Tarjetas de Crédito y Cargo

Ofertas de Protección por Pérdida de Tarjeta de Crédito: Son un Verdadero Robo

Tarjetas de Crédito, Débito y ATM: Qué Hacer si Se Pierden o Son Robadas

Transacciones Bancarias Electrónicas

Facturación Imparcial de Crédito

Su Acceso a Informes de Crédito Gratuitos

Cobranza Imparcial de Deudas

Uso Compartido de Archivos. Cómo Evaluar los Riesgos

Cómo Evitar que lo 'Pesquen' con una Red de Estafa Electrónica

Cómo Disputar Errores en los Informes de Crédito

Spyware

POLÍTICA DE PRIVACIDAD DE LA FTC

Para comunicarse con nosotros, ya sea para presentar una queja o para solicitar información, puede hacerlo a través del Internet, **ftc.gov/robodeidentidad**; telefónicamente llamando a la línea gratuita 1-877-ID-THEFT (1-877-438-4338); o por correo, escribiendo a: Federal Trade Commission, Identity Theft Clearinghouse, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

La FTC ingresa la información que usted envía a su base de datos centralizada de casos de robo de identidad llamada *Identity Theft Clearinghouse* — que es un sistema electrónico de registro cubierto por la Ley de Privacidad del año 1974. En términos generales, la Ley de Privacidad prohíbe la revelación no autorizada de los registros que están bajo su protección. También les brinda a los individuos el derecho de revisar los registros que se mantienen bajo sus nombres. Infórmese sobre sus derechos bajo la Ley de Privacidad y los procedimientos de la FTC relacionados con esta ley comunicándose con la oficina que maneja el acceso libre a la información (*Freedom of Information Act Office*): 202-326-2430; **ftc.gov/foia/privacy_act.htm**.

La información presentada por usted es compartida con los abogados e investigadores de la FTC. Su información también puede ser compartida con empleados de varias otras autoridades federales, estatales o locales de cumplimiento de ley o regulación y también con ciertas entidades

privadas, como compañías de informes de los consumidores y aquellas compañías sobre las cuales usted pudo haber presentado una queja, en caso de que creamos que al hacerlo estamos colaborando en la resolución de problemas relacionados con el robo de identidad. Usted puede ser contactado por la FTC o por cualquiera de las agencias o entidades privadas a las cuales se haya derivado su queja. En algunos casos, entre los que se encuentran las peticiones efectuadas por el Congreso, se nos puede requerir por ley que revelemos la información que usted nos brinde.

Usted tiene la opción de enviar su información anónimamente. Sin embargo, si usted no suministra su nombre e información de contacto, las agencias a cargo del cumplimiento de la ley y demás organizaciones no podrán comunicarse con usted para obtener información adicional que podría ser de ayuda para las investigaciones y procesamientos relacionados al robo de identidad.

NOTAS:

1-877-ID-THEFT (1-877-438-4338)

ftc.gov/robodeidentidad