¿Le han robado su identidad? No está solo.

Millones de personas son víctimas del robo de identidad cada año, lo que genera un considerable sufrimiento emocional y financiero. El aumento de las transacciones digitales y los servicios en línea ha facilitado que los criminales accedan a la información personal, a menudo sin el conocimiento de la víctima. A veces, esto no es algo que usted pueda prevenir fácilmente. Sus datos personales pueden ser robados o filtrados por grandes empresas. Los ladrones pueden obtener esta información personal y usarla para hacerse pasar por usted.

¿Qué es el robo de identidad?

El robo de identidad ocurre cuando alguien roba su identidad para cometer fraude. Los datos de la Comisión Federal de Comercio muestran que en 2023 hubo 917,315 informes de robo de identidad en los Estados Unidos. El robo de identidad ocurre de diversas maneras. Los métodos más comunes incluyen:

- Phishing, donde los estafadores se hacen pasar por organizaciones legítimas para engañar a las personas y que estas proporcionen información sensible;
- Brechas de seguridad, donde los ciberataques a empresas resultan en el robo de datos personales;
- Skimming, donde dispositivos capturan información de tarjetas en cajeros automáticos o sistemas de punto de venta.

El robo de correo, las tácticas de ingeniería social, las vulnerabilidades en redes Wi-Fi públicas y los sitios web falsos también representan riesgos

importantes.

Cuando alguien roba su identidad para cometer fraude, significa que están utilizando su información personal sin su permiso, como:

- Su nombre
- Su número de seguridad social o de Medicare
- El número de su tarjeta de crédito
- Su dirección
- Su fecha de nacimiento

Los ladrones de identidad pueden alquilar apartamentos, obtener tarjetas de crédito, recibir beneficios gubernamentales o reembolsos de impuestos, o abrir otras cuentas a su nombre. Es posible que usted no se entere del robo de identidad hasta que revise su informe de crédito o un estado de cuenta de tarjeta de crédito y note cuentas que no abrió, cargos que no realizó, o hasta que sea contactado por un cobrador de deudas.

¿Estoy en riesgo de robo de identidad?

El robo de identidad puede ocurrirle a cualquiera. Sin embargo, cuanto más información proporcione de manera accesible en línea, incluida la información sobre sus hijos, como compartir públicamente la fecha de nacimiento y el nombre completo de su hijo, más fácil será para los criminales robar una identidad.

Aquí le presentamos algunas maneras de proteger su información personal:

- Almacene la información personal de manera segura en un lugar adecuado. Destruya documentos antes de desecharlos.
- No comparta su número de seguridad social con alguien que lo contacte. Las organizaciones legítimas que podrían necesitar su número de seguridad social generalmente no se comunican con usted

primero. Además, no proporcione su número de seguridad social en solicitudes de empleo en línea. Espere hasta tener una oferta y verifique que la empresa sea legítima.

- Proteja su información en línea y en su teléfono. Asegúrese de usar una contraseña. Las contraseñas fuertes tienen:

    - Al menos 12 caracteres. Intente usar una frase o una combinación de palabras que solo tenga sentido para usted.
    - Una combinación de letras mayúsculas y minúsculas, números y caracteres especiales.
    - No use información personal.
    - También es importante usar contraseñas diferentes y únicas para diferentes sitios web y necesidades. Una forma de hacerlo es asociar de manera libre el tipo de cuenta con una contraseña.
        - Por ejemplo, si tiene una cuenta en una tienda de comestibles y su tipo favorito de fruta es la manzana, específicamente la Honeycrisp, y empezó a ir a esta tienda en 2019, su contraseña podría ser: HONEYcrispCOMEDOR!2019
        - Si tiene una cuenta con un banco local y usa esa cuenta bancaria para pagar sus préstamos de automóvil para su Toyota Camry 2014, y el color del logo del banco es azul marino, su contraseña podría ser: azulmarinoTOYOTAconductora2014$
    - Evite usar fechas de nacimiento, nombres de familiares, incluidos los de mascotas, contraseñas predeterminadas o contraseñas comunes como "contraseña" o "12345678". Mantenga sus cuentas en redes sociales privadas.

    - Si usted es un influencer o decide compartir públicamente sus redes sociales, tenga cuidado con cuánta información comparte,

especialmente información sobre cualquier niño menor de edad.

Si ha sido víctima del robo de identidad, visite IdentityTheft.gov, el recurso único del gobierno federal para ayudarle a reportar y recuperarse del robo de identidad. IdentityTheft.gov le permite reportar el robo de identidad, además de recibir un Informe de Robo de Identidad y un plan de recuperación personal que le guía paso a paso sobre qué hacer. Por ejemplo, puede ponerse en contacto con las compañías de informes crediticios nacionales para recibir ayuda con la colocación de alertas de fraude o congelación de seguridad y bloquear o eliminar deudas fraudulentas.

Alertas de Fraude y Congelaciones de Crédito

No tiene que ser víctima de un robo de identidad para colocar alertas de fraude o congelaciones de seguridad en su cuenta.

Una alerta de fraude de crédito y una congelación de crédito son herramientas importantes diseñadas para proteger a los consumidores del robo de identidad, pero sirven para propósitos diferentes y funcionan de maneras distintas. Una alerta de fraude es una notificación colocada en su informe de crédito que advierte a los posibles acreedores que tomen medidas adicionales para verificar su identidad antes de otorgar crédito.

Típicamente, una alerta de fraude dura 90 días, puede ser extendida y se inicia a través de una de las tres agencias de crédito principales: Equifax, Experian o TransUnion. Cuando coloca una alerta de fraude, la agencia notificará a las otras. Es importante saber que una alerta de fraude no afecta su puntaje de crédito; simplemente actúa como una medida preventiva para los acreedores.

Por otro lado, una congelación de crédito restringe el acceso a su informe de crédito, lo que hace que sea imposible que nuevos acreedores accedan a su información sin su consentimiento. Una congelación puede ser colocada y levantada en cualquier momento, dándole control total sobre cuándo se puede acceder a su informe de crédito. Al igual que una alerta de fraude, una congelación de crédito no afecta su puntaje de crédito, ya que previene el acceso no autorizado, pero no impacta las

cuentas existentes ni la utilización de su crédito.

Si decide solicitar un préstamo o cualquier otro crédito, puede levantar temporalmente una congelación de crédito. Esto puede hacerse en línea, por teléfono o por correo, dependiendo de la agencia de crédito. Tendrá que proporcionar el PIN o la contraseña asociada con la congelación para levantarla. El PIN o la contraseña será establecido por usted o la agencia de informes crediticios le enviará una copia.

En resumen, aunque tanto las alertas de fraude como las congelaciones de crédito ayudan a proteger contra el robo de identidad, funcionan de manera diferente. Una alerta de fraude alienta a los acreedores a verificar la identidad, mientras que una congelación de crédito restringe completamente el acceso a su informe de crédito. Ninguna de las dos acciones afecta su puntaje de crédito, y una congelación de crédito puede levantarse temporalmente cuando solicite un préstamo, tarjeta de crédito o cambie de cuenta bancaria.

Pasos a Seguir

La sección "Pasos" de IdentityTheft.gov ha organizado convenientemente los pasos a seguir si usted es víctima del robo de identidad relacionado con impuestos, salud o niños:

Paso 1 - Llame a las empresas donde sabe que ocurrió el fraude:

- Llame al departamento de fraudes. Explique que alguien robó su identidad.
- Pídales que cierren o congelen las cuentas. Así, nadie podrá añadir nuevos cargos sin su consentimiento.
- Cambie los inicios de sesión, contraseñas y PIN de sus cuentas.

Paso 2 - Coloque una alerta de fraude y obtenga sus informes de crédito:

- Coloque una alerta de fraude gratuita por un año contactando a una de las tres agencias de crédito. Esa compañía debe notificar a las otras dos:

En línea	**Por teléfono**	**Por correo**
Equifax Alerts	(800) 685-1111	Equifax Consumer Fraud Division, P.O. Box 740256, Atlanta, GA 30374
Experian Fraud Center	(888) 397-3742	Experian, P.O. Box 9554, Allen, TX 75013
Transunion Fraud Alert	(888) 909-8872	TransUnion Fraud Victim Assistance Department, P.O. Box 2000, Chester, PA 19016

Además usted puede consultar su informe de crédito para determinar si alguien ya ha hecho algo con su identidad. Obtenga sus informes de crédito gratuitos de Equifax, Experian y TransUnion. Vaya a annualcreditreport.com o llame al 1-877-322-8228.

Paso 3 - Reporte el robo de identidad a la FTC:

- Complete el formulario en líneao llame al 1-877-438-4338. Incluya tantos detalles como sea posible.
- Si crea una cuenta, el FTC lo guía a través de cada paso de recuperación, actualiza su plan según sea necesario, rastrea su progreso y rellena automáticamente formularios y cartas para usted.

- Si no crea una cuenta, debe imprimir y guardar su Informe de Robo de Identidad y plan de recuperación de inmediato. Una vez que salga de la página, no podrá acceder ni actualizarlos.

También puede optar por presentar un informe ante la policía local:

- Vaya a la estación de policía local con:
  - Una copia de su Informe de Robo de Identidad de la FTC
  - Una identificación emitida por el gobierno con foto
  - Prueba de su dirección (estado de cuenta hipotecario, contrato de arrendamiento o factura de servicios públicos)
  - Cualquier otra prueba que tenga del robo (facturas, avisos del IRS, etc.)
- Informe a la policía que alguien robó su identidad y que necesita presentar un informe.
- Solicite una copia del informe policial. Puede que la necesite para completar otros pasos.

Bloqueo o eliminación de información fraudulenta de su informe de crédito

Si ha sido víctima de robo de identidad, también usted puede solicitar a las agencias de informes crediticios que eliminen la información y las deudas fraudulentas de su informe de crédito, lo que se llama bloqueo. Para hacerlo, debe enviar a las agencias de informes crediticios:

- Un informe de robo de identidad, que puede hacerlo a través de IdentityTheft.gov
- Prueba de su identidad
- Una carta identificando las deudas fraudulentas e información en su informe de crédito

A través de IdentityTheft.gov, también puede obtener una carta de muestra para enviar a las agencias de informes crediticios. Recuerde que los informes de robo

de identidad solo se pueden usar para deudas que sean resultado del robo de identidad. Las agencias de informes crediticios pueden negarse a bloquear o rescindir un bloqueo si hace una declaración material falsa sobre ser víctima de robo de identidad o si obtuvo bienes, servicios o dinero como resultado de la transacción bloqueada.

Dentro de los cuatro días hábiles después de recibir su solicitud, la agencia de informes crediticios debe bloquear esa información de su informe de crédito. Además, deben informar a las empresas que proporcionaron la información que alguien robó su identidad. Una vez que se notifique, los acreedores no podrán enviar las deudas relacionadas con el robo de identidad a cobradores de deudas.

Si necesita disputar una deuda que no es el resultado de un robo de identidad, lea ¿Cómo disputar un error en mi informe de crédito?

Si tiene un problema con el informe de crédito, puede presentar una queja ante la CFPB (Oficina de Protección Financiera del Consumidor).

Más sobre las alertas de fraude y los congelamientos

Como recordatorio breve, una alerta de fraude requiere que los acreedores, al revisar su informe de crédito, tomen medidas para verificar su identidad antes de abrir una nueva cuenta, emitir una tarjeta adicional o aumentar el límite de crédito en una cuenta existente a solicitud del consumidor. Cuando usted coloca una alerta de fraude en su informe de crédito en una de las principales agencias de informes de crédito, esta debe notificar a las demás.

Existen dos tipos principales de alertas de fraude: alertas de fraude iniciales y alertas extendidas. Los miembros de las fuerzas armadas también tienen la opción de una alerta de servicio activo.

Alertas de fraude iniciales

Usted puede colocar una alerta de fraude inicial en su informe de crédito si cree que es víctima o está a punto de ser víctima de fraude o robo de identidad. Las agencias de informes de crédito mantendrán esta alerta en su archivo durante un año. Después de un año, la alerta de fraude inicial expirará y será retirada. Usted tiene la opción de colocar otra alerta de fraude en ese momento.

Cuando usted coloca una alerta de fraude inicial, los acreedores deben tomar medidas razonables para asegurarse de que la persona que haga una nueva solicitud de crédito a su nombre sea usted, antes de otorgar dicha solicitud. Si usted proporciona un número telefónico, el acreedor debe llamarlo o tomar medidas razonables para verificar si realmente es usted quien está haciendo la solicitud de crédito antes de aprobarla.

Cuando usted coloca una alerta de fraude inicial en su archivo, tiene derecho a solicitar una copia gratuita de su informe de crédito de cada una de las principales agencias de informes de crédito. Estos informes gratuitos no cuentan como su informe anual gratuito de cada agencia.

Si su identidad ha sido robada y ha presentado un informe de robo de identidad en IdentityTheft.gov, usted puede colocar una alerta extendida en su informe de crédito.

Alerta extendida

Una alerta extendida es válida por siete años. Si usted tiene una alerta extendida, el acreedor debe contactarlo en persona, por teléfono o a través de otro método de contacto que usted elija para verificar si realmente es usted quien está haciendo la solicitud de crédito antes de otorgar un nuevo crédito.

Cuando usted coloca una alerta de fraude extendida en su archivo, tiene derecho a solicitar dos copias gratuitas de su informe de crédito de cada agencia de informes de crédito durante un período de 12 meses. Su nombre también será removido durante cinco años de las listas de marketing preseleccionado de las agencias de informes de crédito para ofertas de crédito y seguros.

Alertas de servicio activo

Los miembros de las fuerzas armadas tienen una opción adicional disponible para ellos: alertas de servicio activo, que protegen a los miembros del servicio mientras están en servicio activo y asignados fuera de su lugar de trabajo habitual. Esta alerta requiere que las empresas tomen medidas razonables para verificar su identidad antes de emitir crédito a su nombre. Estas alertas duran 12 meses, a menos que usted solicite que la alerta sea retirada antes. Si su despliegue dura más de 12 meses, puede colocar otra alerta en su archivo de crédito.

Cuando usted coloca una alerta de servicio activo en su informe de crédito, los acreedores deben tomar medidas razonables para asegurarse de que la persona que hace la solicitud de crédito sea usted antes de abrir una cuenta, emitir una tarjeta de crédito adicional o aumentar el límite de crédito en su cuenta existente. Su nombre también será removido durante dos años de las listas de marketing preseleccionado de las agencias de informes de crédito para ofertas de crédito y seguros.

Dado que puede ser muy difícil contactarlo directamente si está desplegado, usted puede asignar a un representante personal para que responda por usted o para colocar o retirar una alerta de servicio activo.

Este artículo fue recopilado de fuentes como la Oficina de Protección Financiera del Consumidor y la Comisión Federal de Comercio, y editado por LawNY.

****

Asistencia Legal de Western New York, Inc. ®

Este artículo proporciona información general sobre este tema. Las leyes que afectan este tema pueden haber cambiado desde quese escribió su artículo. Para obtener asesoramiento legal específico sobre un problema que está teniendo, obtenga el asesoramiento de un abogado. Recibir esta información no lo convierte en cliente de Legal Assistance of Western New York, Inc.

Fecha de la última revisión: noviembre de 2024

Last updated on November 26, 2024.

Articulos en Espanol
Legal Information Article
Print

Table of Contents

NEWS

News & publications

The news about recent activities for needed peoples.

More News

13 Nov 2024

Surprisingly High Utility Bill? The Utility May be Back-billing You

Para ver este artículo en español por favor visite aquí. (To view this article…

Continue Reading

1 Nov 2024

Notice of LawNY Board Meeting

The next meeting of the LawNY Board of Directors is scheduled for December 17,…

Continue Reading