Robos de identidad

¿Qué es el robo de identidad?

Se trata del uso deliberado de la identidad de otra persona, y se da cuando alguien emplea los datos personales de otra persona, como el nombre, el número de seguro social o el número de cuenta bancaria, sin su permiso para hacer fraudes o cometer otros delitos. Algunos ejemplos son el uso del nombre y la información de identificación personal para abrir cuentas bancarias, crear nuevas cuentas de tarjetas de crédito, falsificar cheques y hasta obtener préstamos. Algunos indicios de que le pueden haber robado la identidad son la no recepción de facturas u otros documentos que esperaba por correo postal, la recepción de tarjetas de crédito que no solicitó, el rechazo de crédito por motivos no evidentes, y la recepción de llamadas de cobradores de deudas o empresas en relación con bienes o servicios que usted no compró. Si bien es imposible asegurarse de nunca sufrir un robo de identidad, existen medidas que pueden tomarse para reducir los riesgos.

¿Cómo se dan los robos de identidad?

Los ladrones de identidades emplean una serie de métodos para robar información de identificación personal, por ejemplo:

- Robo de basura: Los ladrones revuelven la basura en busca de facturas u otros documentos con datos personales.
- Robo de correo postal: Los ladrones revisan el correo en busca de estados de cuenta bancarios y tarjetas de crédito, ofertas de tarjetas de crédito preaprobadas, información fiscal y demás documentos que puedan incluir datos personales.
- Dispositivo: Mediante un dispositivo de almacenamiento especial, se puede robar el número de la tarjeta de crédito/débito al procesarla.
- Phishing: Se trata de una estafa de ingeniería social en la que por correo electrónico se engaña al usuario para que revele datos personales.
- Cambio de domicilio: Los delincuentes suelen desviar recibos a otro lugar al completar un formulario de cambio de domicilio.
- Robo físico: Consiste en robar billeteras, bolsos y correo postal, donde pueden hallar ofertas de tarjetas de crédito preaprobadas, estados de cuenta bancarios o chequeras.
- Pretexting: Fraude de ingeniería social por la cual un delincuente se hace pasar por otra persona para obtener datos personales de alguien.
- Robo de datos: Robo electrónico de registros de datos.

Protección de la información de identificación personal

Third Coast Bank SSB tiene procedimientos para proteger y monitorear las cuentas y la información de identificación personal de los clientes. Estos son algunos consejos para reducir el riesgo de que le roben la identidad:

- Proteja su número de seguro social: No lleve la credencial de seguro social en la billetera ni anote el número en cheques. Dígalo solo cuando sea necesario.
- Triture los documentos: Triture los datos y documentos financieros y la información personal antes de desecharlos.
- Revise su informe de credito: Una ley federal exige a las principales agencias nacionales de calificación crediticia (Equifax, Experian y TransUnion) entregarle una copia gratuita de su informe de credito cada 12 meses si usted la solicita. Visite www.AnnualCreditReport.com para solicitar su copia gratuita.
- Nunca haga clic en enlaces de mensajes de correo electrónico no solicitados: Hay que eliminar los mensajes donde se soliciten datos de cuentas, información de identificación personal o contraseñas. Pueden tratarse de estafas de phishing.

- Proteja sus contraseñas: Utilice contraseñas difíciles de adivinar y memorícelas. No emplee códigos previsibles, como su fecha de nacimiento, el apellido de soltera de su madre, o su número de seguro social. No le diga las contraseñas a nadie.
- Monitoree sus estados financieros: Monitoree con atención y regularidad en la banca en línea sus cuentas bancarias, financieras y de tarjetas de crédito, en busca de cobros no autorizados. Reporte de inmediato toda actividad sospechosa a su banco o institución financiera.
- Proteja su información de identificación personal: Los datos personales no protegidos pueden correr peligro.
    - No dé información de identificación personal por teléfono, mensaje de texto, correo electrónico o Internet, al menos que usted haya iniciado la comunicación y este al tanto con quién está tratando.
    - No utilice WIFI ni conexiones inalámbricas públicas.
    - Guarde y deseche de forma segura la información de identificación personal.
    - No comparta información de más en las redes sociales.

¿Qué debe hacer si es víctima de un robo de identidad?

Se recomienda seguir estos pasos, en cuanto tome conocimiento del robo de identidad.

- Comuníquese con sus instituciones financieras: Comuníquese con Third Coast Bank SSB de inmediato si la actividad fraudulenta está relacionada con sus cuentas bancarias. Revise la actividad de todas sus cuentas, incluyendo las cuentas de cheques y de ahorro, las de tarjetas de débito, las de préstamos y todas las demás cuentas bancarias, en busca de modificaciones de domicilio, cambios de números de identificación personal (NIP) o solicitudes de tarjetas nuevas. Notifique sobre el posible fraude al departamento de fraudes de las empresas de tarjetas de crédito y demás bancos y entidades crediticias. Cierre las cuentas que sepa o crea que se hayan modificado o abierto de modo fraudulento. Cambie de inmediato su nombre de usuario y contraseña de la banca en línea.
- Comuníquese con la policía: Llame de inmediato a la policía local o a la policía de la comunidad donde se haya producido el robo de identidad para hacer la denuncia. La policía puede iniciar una investigación y usted puede obtener información de la denuncia policial, la cual probablemente necesite para resolver problemas con sus cuentas y su informe crediticio.
- Complete un formulario de declaración jurada: Las instituciones financieras y las fuerzas de seguridad pueden exigirle que complete un formulario de "denuncia y declaración jurada como víctima de robo de identidad". La Comisión Federal de Comercio (FTC) creó el formulario de declaración jurada para las víctimas de robos de identidad. Usted puede ir a https://www.identitytheft.gov/ para reportar el robo de identidad y acceder a un plan de recuperación.
- Comuníquese con las agencias de calificación crediticia: Llame a la línea gratuita de atención de cualquiera de las tres principales agencias a continuación para generar una "alerta de fraude" para su informe de credito. Solo necesitará comunicarse con una de las tres agencias, ya que la primera agencia que contacte reportará la situación a las demás.

Equifax:	1.800.525.6285	www.equifax.com
Experian:	1.888.397.3742	www.experian.com
TransUnion:	1.800.680.7289	www.transunion.com

- Solicite que en el informe se indique a las entidades crediticias que se comuniquen con usted para confirmar futuras solicitudes de crédito. Una vez emitida la alerta de fraude, tendrá derecho a una copia gratuita de su informe de credito de cada una de las agencias. Revise con atención cada informe de credito que reciba. Busque consultas de empresas que no haya contactado, cuentas que no haya abierto, y deudas para las que no tenga explicación. Siga revisando sus informes de credito periódicamente para asegurarse de que no haya actividades fraudulentas nuevas.
- Comuníquese con la Comisión Federal de Comercio: Reporte la actividad delictiva a la FTC mediante el formulario para denuncias en línea o llamando a la Línea para robos de identidad al 1-877-ID-THEFT (438-4338) para hablar con un asesor especializado en robos de identidad.
- Notifique a las empresas de verificación de cheques: Muchos comercios minoristas emplean importantes empresas de verificación de cheques, así que debería contactar a su banco y pedir que se reporte la información de su cuenta al Sistema de Notificación de Cierre de Cuentas (CANS) de Texas. Al hacer esto,

todas las principales entidades de verificación de cheques tendrán acceso a la información y reportarán la estafa a los comercios que empleen sus servicios. Para acceder al formulario exigido por su institución financiera para ingresar la información en la base de datos, visite el sitio web https://www.dob.texas.gov/public/uploads/files/Applications-Forms-Publications/Applications-Forms/cve_ssfininst.pdf.

- Deje registrada la información: Anote los nombres, los teléfonos y las fechas de cada persona con la que hable sobre el incidente. Puede descargar e imprimir el formulario de "Seguimiento del proceso" para registrar todos los pasos dados al reportar el robo de identidad. Envíe cartas a todos los lugares con los que haya hablado por teléfono y guarde copias de toda la correspondencia.
- Siga revisando todas las cuentas: Dado que los robos de identidad pueden demorar en resolverse, revise atentamente todos los cobros y las transacciones que aparezcan en sus estados de cuentas y en línea. Reporte las discrepancias de inmediato.

Si cree haber sido víctima de un robo de identidad, comuníquese con un representante del banco lo antes posible para que podamos tomar las precauciones adecuadas y ayudarlo.

Para tener en cuenta: Este documento no incluye los enlaces. Deberá copiar los enlaces y pegarlos en otra ventana del navegador para visitar los sitios web.