KIT DE PROTECCIÓN CONTRA EL ROBO DE IDENTIDAD DE CHASE

Su seguridad es importante para nosotros. Utilice esta guía para obtener más información acerca del robo de identidad, para protegerse, y para recuperarse si ya ha sido víctima.

Para hablar con nuestro Grupo de Protección al Cliente, llame al 1-888-745-0091; aceptamos llamadas de retransmisión con operador.

¿QUÉ ES EL ROBO DE IDENTIDAD?

El robo de identidad ocurre cuando un delincuente obtiene su información personal e intenta robar dinero de sus cuentas, abrir nuevas tarjetas de crédito, solicitar préstamos, alquilar apartamentos, y cometer otros delitos, todo esto utilizando su identidad. El robo de identidad puede dañar su crédito, dejarlo con facturas no deseadas, y requerir mucho tiempo y frustración para lograr solucionarlo.

REQUISITOS PARA SOLICITAR DOCUMENTACIÓN DE LA TARJETA DE CRÉDITO

Nos damos cuenta de que usted puede ser víctima de robo de identidad de la tarjeta de crédito y que quisiera detalles de una solicitud de tarjeta de crédito o archivos comerciales de la cuenta. Antes de que podamos enviarle detalles específicos de cualquier solicitud o archivo comercial, la ley FACT de 2003 y nuestras propias políticas de protección de identidad nos requieren obtener la siguiente información de su parte:

- Una copia legible de una identificación emitida por el gobierno. Podemos aceptar una licencia de conducir emitida por el estado, una identificación militar, una tarjeta de identificación del estado o un pasaporte.
- Un informe de robo de identidad completado y firmado o un formulario de fraude por robo de identidad y declaración de falsificación. Para su comodidad, puede:
    - Completar el informe de robo de identidad por internet en el sitio web de la Comisión Federal de Comercio (FTC) en identitytheft.gov.
    - Llamar al 1-877-IDTHEFT (1-877-438-4338) para solicitar el informe de robo de identidad de la FTC.
    - Obtener un formulario de fraude de robo de identidad y declaración de falsificación en su sucursal de Chase o cualquier institución financiera.
- Una solicitud por escrito de una copia de la solicitud que incluya un resumen de toda la información relevante acerca del robo de identidad.
- Documentación de terceros, si corresponde. Los ejemplos incluyen papeleo aprobado del poder legal (power of attorney, POA), curador, tutor, fideicomisario o albacea.

Todas las solicitudes por escrito deben enviarse mediante correo postal de primera clase a:

Chase Card Services
ATTN: FACT Act Request
PO Box 15941
Wilmington, DE 19885-9918

CÓMO OCURRE EL ROBO DE IDENTIDAD

Hoy en día, cada dispositivo con acceso a internet y sitio web que utilice podría estar en riesgo, especialmente cuando configura o utiliza cuentas que requieren información personal.

A través de dispositivos electrónicos e Internet

- Suplantación de identidad (phishing), (se pronuncia "fishing"): usted recibe un correo electrónico de aspecto confiable, pero le solicita llamar a un número fraudulento, responder al correo electrónico o ir a un sitio web e ingresar información personal. Recuerde, ningún representante legítimo de JPMorgan Chase le solicitará jamás su PIN o contraseña por correo electrónico. Solo le pediremos esa información por teléfono.
- Suplantación de identidad (spoofing): sitios web falsos que se ven legítimos y le piden proporcionar información personal.
- Robo de datos (Pharming): esto puede suceder cuando ingresa a un sitio web legítimo, pero su navegador es dirigido a una ubicación falsa de aspecto similar para obtener su información personal.
- Hacking: hay varias técnicas que utilizan los ladrones para instalar programas maliciosos en sus dispositivos. Los programas capturan sus pulsaciones en el teclado y el tráfico de red para robar información personal, incluidas su identificación de usuario y contraseñas.
- Robo: si se apoderan de su computadora portátil, teléfono inteligente u otro dispositivo, los ladrones pueden usar datos no asegurados para descubrir contraseñas y acceder a las cuentas.
- Skimming: obtención de números de tarjeta de débito y crédito utilizando un dispositivo especial en cajeros automáticos o cuando se procesa una compra.

A través de su correo postal y documentos personales

- Encontrando información personal en su hogar.
- Robando billeteras y bolsos con su identificación y tarjetas bancarias.
- Apoderándose de su correo postal, incluyendo los estados de cuenta de su tarjeta de crédito y bancarios, ofertas de crédito preaprobadas, tarjetas para llamadas telefónicas e información de impuestos.
- Completando un “formulario de cambio de dirección” para desviar su correo postal a otra ubicación.
- Hurgando en la basura en busca de datos personales, también conocido como "dumpster diving".
- Obteniendo su informe de crédito haciéndose pasar por alguien que tiene una necesidad legítima y un derecho legal a obtener la información.

CÓMO UTILIZAN LOS LADRONES SU INFORMACIÓN PERSONAL

Llaman a su banco y cambian su dirección de correo postal
Los ladrones pueden hacerse pasar por usted y cobrar cargos en su cuenta. Es posible que no sepa que hay un problema porque los estados de cuenta se envían a la nueva dirección.

Pueden abrir nuevas tarjetas de crédito y cuentas bancarias a su nombre
Todo lo que puede que necesiten es su nombre, fecha de nacimiento y número de Seguro Social (SSN). Cuando utilizan la tarjeta de crédito y no pagan las facturas, la cuenta en incumplimiento de pago se informa en su informe de crédito.

También podrían registrarse para un servicio de teléfono o de telefonía celular, falsificar cheques o tarjetas de débito, y comprar automóviles adquiriendo un préstamo para automóvil a su nombre.

CÓMO MANEJAR EL ROBO DE IDENTIDAD

Si usted es víctima de robo de identidad, así es como puede recuperarse. Para ver una lista de verificación y cartas de ejemplo que le guiarán en el proceso de recuperación, visite IdentityTheft.gov.

1. Notifique a todos sus bancos y compañías financieras tan pronto se percate de que le han robado su identidad o de que su cuenta está en riesgo.
   - Si realiza operaciones bancarias con nosotros, llame a nuestro Grupo de Protección al Cliente al 1-888-745-0091.
   - Trabajaremos con usted para ayudarle a corregir cualquier transacción no autorizada en sus cuentas de Chase, corregir cualquier información incorrecta que hayamos enviado a las agencias de informes de crédito y ayudar a protegerle de cualquier futuro robo de identidad o fraude en la cuenta.

2. Solicite a las agencias de informes de crédito que coloquen una alerta de fraude o bloqueo de crédito en su archivo crediticio. Estas agencias mantienen los informes que realizan el seguimiento de las cuentas de crédito abiertas a su nombre.
   a. Un bloqueo de crédito, también conocido como “bloqueo de seguridad”, evita que los acreedores accedan a su informe de crédito. Esto hace que sea más difícil para los ladrones de identidad abrir cuentas a su nombre. Eso es porque la mayoría de los acreedores tienen que ver su informe de crédito para aprobar una nueva cuenta.

3. Revise detenidamente sus informes de crédito.
   a. Usted tiene derecho a obtener un informe de crédito gratis cada año de cada una de las tres principales agencias de informes de crédito: Equifax, Experian y TransUnion. Obtenga más información y solicite el suyo hoy mismo en AnnualCreditReport.com.
   - Busque todas las cuentas fraudulentas y los cambios no autorizados.
   - Revise la sección de consultas en busca de cuentas o solicitudes fraudulentas. Si ve alguna, solicite a la agencia que enmascare o elimine la consulta. Solo usted podrá visualizar una consulta enmascarada.

4. Presente una denuncia ante la policía local, incluida la comunidad donde se produjo el robo de identidad.
   - Puede darles una copia a los acreedores como prueba del fraude
   - Si la policía no puede presentar un informe de robo, solicíteles que presenten un informe de incidente misceláneo.

5. Informe cualquier problema con su correo postal y confirme su dirección.
   - Si recibe estados de cuenta para cuentas que usted no abrió, comuníquese con el acreedor.
   - Si no recibe estados de cuenta de sus cuentas habituales, comuníquese con el banco u otra compañía.
   - Si no recibe correo postal normal, comuníquese con su oficina de correo local.

6. Cierre las cuentas que se abrieron, cambiaron o donde se realizaron cargos de forma fraudulenta. Revise todas sus cuentas, incluidas tarjetas de crédito, cuentas bancarias y servicios públicos.
   a. Si ve actividad sospechosa, comuníquese con el acreedor, el banco o la compañía de servicios públicos.
   b. Si abre cuentas nuevas después de eso, utilice nuevos PIN y contraseñas.
   - Si se robaron cheques o si estos se utilizaron de forma indebida, infórmeles a las compañías de verificación de cheques.
     - TeleCheck: 1-800-710-9898
     - Certegy: 1-800-437-5120
   - Si alguien configuró un nuevo teléfono o servicio de telefonía celular a su nombre, solicite al proveedor de servicio que cancele la cuenta. Si no la cancelan, comuníquese con la Comisión Estatal de Servicios Públicos (State Public Utilities Commission) de los proveedores de servicio locales o con la Comisión Federal de Comunicaciones (Federal

Communications Commission) en FCC.gov. Para proveedores de servicio de larga distancia, llame al 1-888-CALL-FCC (1-888-225-5322).

- Si alguien utilizó su número de Seguro Social (SSN) para solicitar un empleo, llame a la línea directa de fraude del Seguro Social al 1-800-269-0271. Para confirmar la precisión de las ganancias informadas en su estado de cuenta de Seguro Social, llame a la Administración del Seguro Social al 1-800-772-1213.
- Si alguien utilizó su nombre para obtener una licencia de conducir o una tarjeta de identificación, o si su licencia de conducir se perdió o fue robada, comuníquese con su Departamento de Vehículos Motorizados local.

FRAUDE A TRAVÉS DE LA COMPUTADORA E INTERNET

Si el fraude se produjo a través de su computadora, estas son algunas de las medidas que puede tomar.

Si esto sucede	Esto es lo que puede hacer
Hacking (instalación de programas maliciosos) y virus de computadora	Comuníquese con su proveedor de servicios de internet y con el FBI en IC3.gov.
Fraude a través de Internet	Infórmelo a la Comisión Federal de Comercio (FTC) en FTC.gov/complaint. La FTC ingresa los reclamos en una base de datos segura por internet, disponible para cientos de agencias del orden público civiles y criminales en los Estados Unidos y en el extranjero.
Correos electrónicos engañosos o de suplantación de identidad (phishing)	Envíeles cualquier información que tenga a: • spam@uce.gov (FTC), y • reportphishing@antiphishing.org (The Anti-Phishing Working Group). Si ve un correo electrónico sospechoso que parece ser de nosotros, reenvíelo a abuse@chase.com. Le enviaremos una respuesta automatizada para informarle que recibimos el mensaje.
Entregó su información personal a un estafador por equivocación	7. Presente un reclamo en FTC.gov/complaint. 8. Visite FTC.gov/IDTheft para obtener información sobre cómo reducir el daño de robo de identidad.
Tiene sospechas sobre un sitio web de redes sociales	Informe al sitio web de redes sociales acerca de sus inquietudes. La mayoría tiene enlaces donde puede informar inmediatamente comportamiento por internet abusivo, sospechoso o inapropiado.

CÓMO PREVENIR EL ROBO DE IDENTIDAD

Una de las mejores maneras de luchar contra el robo de identidad es, en primer lugar, evitar que suceda. Estas son algunas maneras que pueden ayudar a prevenir que otros roben su información.

Proteja sus dispositivos	• Obtenga más información sobre cómo sus dispositivos guardan contraseñas y números de cuenta. • Confirme que cualquier software que utilice para guardar datos personales sea seguro. • Configure su computadora portátil para requerir una contraseña cuando se inicie o reactive.
Manténgase alerta cuando esté en internet	• Asegúrese de que los sitios web que visita son seguros y protegen sus datos. • Busque sitios web que utilicen tecnología de capa de sockets seguros (SSL) para encriptar su información personal. Verifique un pequeño símbolo de candado en la esquina inferior de su navegador o junto a la URL. • Cree contraseñas seguras y no se las entregue a nadie.

Tenga cuidado con las estafas por teléfono	• Guarde en privado sus cheques nuevos, cancelados y que no se hayan usado. • No proporcione su información personal o financiera por teléfono, incluyendo cuentas de cheques, tarjetas de crédito y números de Seguro Social (SSNs), a menos que esté seguro de que la otra parte es legítima. • Notifique a las instituciones financieras de llamadas telefónicas sospechosas que soliciten información de la cuenta.
Realice un seguimiento de los estados de cuenta mensuales	• Si no le llegan sus estados de cuenta, llame a la compañía para averiguar el motivo y confirme su dirección. • Si sus estados de cuenta tienen transacciones u otros elementos de la factura sospechosos, no los ignore. Investíguelos inmediatamente y comuníquese con su banco o acreedor.
Pruebe los estados de cuenta electrónicos	Estos pueden protegerle contra el robo de identidad y reducir la cantidad de correo postal. La mayoría de los sitios web también le solicitarán su contraseña para que pueda ver los estados de cuenta.
Verifique su informe de crédito	• Usted tiene derecho a obtener un informe de crédito gratis cada año de cada una de las tres principales agencias de informes de crédito. • También puede obtener una copia de su informe de crédito en cualquier momento pagando un cargo. • Si ve cuentas o consultas sospechosas, comuníquese con la agencia.
Manipule cuidadosamente los recibos y el correo postal	• Deseche su correo postal de forma segura. • No tire los recibos de cajero automático y de tarjeta de crédito en botes de basura públicos. • Considere tener un triturador de papel para los documentos confidenciales, como ofertas de mercadeo, estados de cuenta bancarios, documentos, facturas, etc. • Utilice los buzones oficiales de recolección del servicio postal para correo postal saliente o asegure su buzón de correo.
Sea creativo con sus contraseñas y cámbielas con frecuencia	• Las contraseñas más seguras son una combinación de letras, números y caracteres especiales. • Jamás utilice el nombre de su mascota, el nombre de su hijo o hija, ni nada que un estafador pudiera averiguar fácilmente, como su dirección, número de teléfono o fecha de nacimiento. • No utilice información de su cuenta de medios sociales para su contraseña. • Evite utilizar la misma contraseña para varios sitios o instituciones financieras.
Proteja sus PIN y contraseñas	• No escriba su PIN en sus tarjetas de cajero automático o de crédito. • No guarde sus PIN con sus tarjetas. • No comparta PIN ni contraseñas con amigos o familiares.
Lleve con usted solamente lo que necesite	• Mientras menos información personal lleve, en mejor posición estará si le roban su billetera o su cartera.

	• Revise lo que lleva con usted, como su tarjeta médica, ya que puede tener información confidencial como su número de Seguro Social (SSN).
Informe de inmediato cualquier problema	• Informe actividades fraudulentas, tarjetas de crédito robadas o perdidas y cheques no reconocidos. • Asegúrese de que los cheques que se paguen hayan sido emitidos por usted. • Revise los cheques nuevos para garantizar que ninguno se haya robado en tránsito.
No imprima de antemano información personal en los cheques	Sus cheques no deben tener su licencia de conducir, teléfono o número de Seguro Social (SSN).
Sea cuidadoso en los medios sociales	Es mejor ser cuidadoso con la configuración de privacidad y con la información personal que comparte en medios sociales.

CONTACTOS IMPORTANTES

Contactos de Chase
Grupo de Protección al Cliente: 1-888-745-0091
Sitio web: chase.com/IdentityTheft

Para otras preguntas acerca de la cuenta:

Tarjetas de débito	1-800-935-9935
Cuentas de depósito	1-800-935-9935
Hipotecas	1-800-848-9136
Préstamos para automóvil	1-800-336-6675
Arrendamientos para automóvil	1-800-227-5151
Clientes de corretaje	1-800-392-5749
Financiación de la educación	1-800-489-5005
Líneas de crédito sobre el valor líquido de la propiedad	1-800-836-5656

Aceptamos llamadas de retransmisión con operador.

Agencias de informes de crédito

Equifax	1-800-525-6285
Experian	1-888-397-3742
TransUnion	1-800-680-7289

Otros contactos importantes

Comisión Federal de Comercio (FTC)	Para obtener más información acerca del robo de identidad, visite la FTC en FTC.gov/IDTheft o llame al 1-877-ID-THEFT (1-877-438-4338).
Servicio de Inspección Postal de los Estados Unidos	USPIS.gov
Servicio Secreto de los Estados Unidos	Encuentre una oficina local cercana a usted en SecretService.gov.
Línea Directa de Fraude del Número de Seguro Social	1-800-269-0271
Departamento del Seguro Social	1-800-772-1213
Pasaportes perdidos o robados	1-877-487-2778