Guía contra fraude y robo de identidad en línea

Guía de protección de su identidad y de sus cuentas

mkt 44409-06

Como parte del compromiso de SunTrust hacia la protección de sus cuentas y de su identidad, hemos creado la Guía contra fraude y robo de identidad en línea, la que brinda información sobre cómo prevenir el fraude y el robo de identidad a través de Internet, así como las medidas que debe tomar si llegara a convertirse en víctima del robo de identidad.

Aunque podría ser imposible evitar por completo el robo de su identidad y el fraude, puede ayudar a proteger su información personal y sus cuentas con tan sólo seguir las recomendaciones incluidas en esta guía.

¿Qué encontrará en el interior?

- ¿Qué es el robo de identidad?
- Ayude a prevenir el robo de identidad
- Esté pendiente de los fraudes en línea
- Ayude a prevenir el fraude en línea
- ¿Cómo salvaguarda SunTrust la información de sus clientes?
- En caso de convertirse en víctima del robo de identidad…
- Obtenga información adicional sobre el fraude y el robo de identidad en línea

¿Qué es el robo de identidad?

El robo de identidad es un delito grave que ocurre cuando una persona obtiene y utliliza, de manera ilícita, información personal de alguien para beneficio propio. Su nombre, dirección, fecha de nacimiento, número de Seguro Social, contraseñas de Servicios Bancarios por Computadora, números de identificación personal (PIN) y números de tarjetas de crédito y de débito son las piezas esenciales de su información financiera. Cuando los delincuentes obtienen esta información, pueden cambiar los gastos cargados a sus cuentas, crear nuevas cuentas a nombre de usted o utilizar su información personal para otros fines ilícitos.

¿Cómo pueden robarle su identidad?

Éstos son algunos ejemplos de la manera en que los delincuentes podrían obtener su identidad:

- Buscar en su basura a fin de encontrar información impresa que no haya sido triturada o destruida de otra manera, tal como ofertas de tarjetas de crédito y facturas o estados de cuenta anteriores.
- Interceptar su correspondencia llenando formularios de cambio de domicilio y recibir correo que está dirigido a usted.
- Robarle su billetera o bolso, que puede contener una gran cantidad de información sobre usted, incluyendo sus números de cuenta, su número de Seguro Social, su dirección y su fecha de nacimiento.
- Copiar sus números de cuenta después de que su tarjeta de crédito es utilizada al efectuar compras utilizando dispositivos de mano especiales.
- Obtener acceso a los archivos de la empresa donde usted trabaja, los que contienen una gran cantidad de información personal y comercial sobre usted.
- Conseguir información directamente de su parte, haciéndose pasar por vendedores telefónicos u otras personas que podrían tener una razón legítima para pedirle información personal (tal como su banco, la compañía donde trabaja o el propietario de su hogar). También utilizan correos electrónicos y sitios web falsos con el objetivo de intentar que usted les proporcione información.

Señales y síntomas del robo de identidad

El robo de identidad es peligroso porque puede ocurrir sin que usted se dé cuenta. A continuación mencionamos algunas circunstancias que podrían ayudarle a saber si ha sido víctima del robo o de un intento de robo de su identidad:

- **Correspondencia extraviada** – Si cree que no le está llegando toda su correspondencia o experimenta una reducción importante en la cantidad de correspondencia que recibe, es posible que sea una víctima de este delito.
- **Transacciones sospechosas** – Vigile sus cuentas, estados de cuenta e informes de crédito a fin de detectar cualquier transacción sospechosa o poco común.
- **Rechazos inesperados** – Esté pendiente de rechazos inesperados al solicitar un préstamo o una hipoteca a pesar de contar con un buen historial de crédito.
- **Llamadas telefónicas extrañas** – Las llamadas de agencias de cobranzas o de un negocio que estén relacionadas con mercancía o servicios que usted no reconoce son otra señal de que alguien podría haberle robado su identidad.
- **Nuevas tarjetas de crédito** – Recibir por correo una tarjeta de crédito que usted no solicitó podría ser una señal de que alguien ha tratado de robarle su identidad.

Ayude a prevenir el robo de identidad

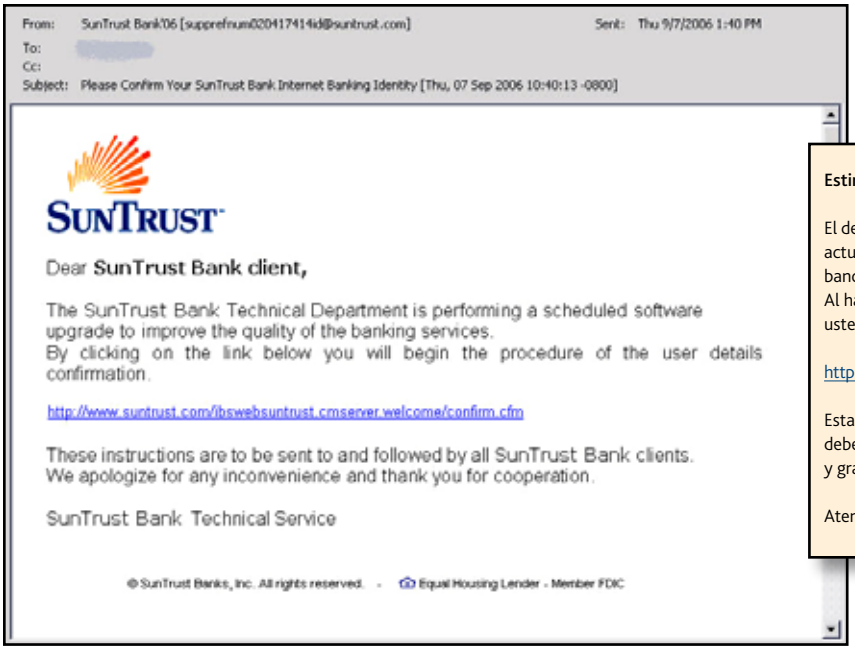
Es importante tener cuidado al divulgar su información personal y financiera. Existe una serie de medidas que puede tomar a fin de protegerse contra el robo de identidad:

- **Firmar el reverso de sus tarjetas de crédito y de débito**. Esto minimiza la posibilidad de que alguien más utilice su tarjeta.
- **Conservar los recibos de sus tarjetas de crédito y de débito**. Úselos para verificar sus estados de cuenta e identificar cualquier actividad sospechosa.
- **Informar de inmediato las tarjetas de crédito o débito que hayan sido robadas o extraviadas**. Si pierde o le roban una tarjeta de crédito o de débito, es importante que se comunique de inmediato con su banco.
- **Cancelar y destruir las tarjetas y cheques que no utiliza**. Deseche las tarjetas de crédito y los cheques que no use. Llame a su banco a fin de cancelar sus tarjetas y destrúyalas antes de desecharlas. Al destruir sus tarjetas y cheques, no olvide cerciorarse de que los números no sean legibles o reconocibles.
- **No escribir información personal en sus cheques**. No necesita incluir su número de licencia para conducir, teléfono o número de Seguro Social en sus cheques. Al omitir esta información, usted evita que la información confidencial caiga en manos indebidas.
- **No dejar su correspondencia al alcance de todos**. La correspondencia que recibe incluye información personal, de manera que asegúrese de recogerla oportunamente.
- **Destruir la correspondencia chatarra que recibe**. Asegúrese de triturar o destruir la correspondencia que recibe antes de desecharla, particularmente las ofertas de tarjetas de crédito, las cuales podrían contener información confidencial.
- **No depositar en su buzón la correspondencia que desea enviar**. Es más seguro depositarla en los buzones del Servicio Postal – particularmente si el buzón de su hogar no está cerrado con llave.
- **Examinar sus informes de crédito**. Cerciórese de que no contengan ningún error. Existen tres agencias dedicadas a la elaboración de informes de crédito, cuyos informes pueden contener información diferente. Lo mejor es examinarlos al menos una vez al año a fin de detectar cualquier actividad irregular o sospechosa.
  - Equifax 800.525.6285 o equifax.com
  - Experian 888.397.3742 o experian.com
  - TransUnion 800.680.7289 o transunion.com
- **No responder a solicitudes de información personal o sobre sus cuentas que usted no haya pedido**. Las solicitudes de información personal a través de correos electronicos o de avisos que aparecen repentinamente en las páginas web pueden ser muy peligrosas. Si la solicitud de información le parece sospechosa, llame a la compañía para asegurarse.
- **Conservar su información personal en un lugar seguro.** No conserve en su cartera ni en su computadora una lista con los números de sus tarjetas de crédito, PIN o contraseñas. Memorice esta información.

Guía contra fraude y robo de identidad en línea

Una forma muy común de fraude a través de Internet recibe el nombre de "phishing" (se pronuncia "fishing", es decir, "pescar" en inglés), y consiste en el uso de mensajes de correo electrónico o de avisos que aparecen repentinamente en las páginas web en los que se le invita a divulgar información personal o sobre sus cuentas. Al responder a estas tretas, usted pone en peligro la seguridad de sus cuentas y su identidad puede ser robada. Nunca debe proporcionar información personal o sobre sus cuentas en respuesta a mensajes de correos electónicos o avisos que aparecen repentinamente en las páginas web que usted no solicitó.

Estos son ejemplos de mensajes de correos electrónicos falsos o fraudulentos:



From: SunTrust Bank106 [supprefnum020417414id@suntrust.com] Sent: Thu 9/7/2006 1:40 PM
To:
Cc:
Subject: Please Confirm Your SunTrust Bank Internet Banking Identity [Thu, 07 Sep 2006 10:40:13 -0800]

SUNTRUST

Dear **SunTrust Bank client,**

The SunTrust Bank Technical Department is performing a scheduled software upgrade to improve the quality of the banking services.
By clicking on the link below you will begin the procedure of the user details confirmation.

http://www.suntrust.com/ibswebsuntrust.cmserver.welcome/confirm.cfm

These instructions are to be sent to and followed by all SunTrust Bank clients.
We apologize for any inconvenience and thank you for cooperation.

SunTrust Bank Technical Service

© SunTrust Banks, Inc. All rights reserved. - Equal Housing Lender - Member FDIC

Estimado cliente de SunTrust Bank,

El departamento técnico de SunTrust Bank está llevando a cabo una actualización de su software para mejorar la calidad de sus servicios bancarios.
Al hacer clic u oprimir en el enlace que se encuentra en la parte inferior, usted comenzará el proceso de de verificación de los detalles del usuario.

http://www.suntrust.com/ibswebsuntrust.cmserver.welcome/confirm.cfm

Estas indicaciones deben enviarse a todos los clientes de SunTrust Bank y deben ser acatadas por éstos. Sentimos la molestia que esto le ocasiona y gracias por su cooperación.

Atención Técnica de SunTrust Bank

AVISO DE CAMBIO DE CORREO ELECTRÓNICO

Estimado(a): _____,

Gracias por efectuar sus operaciones bancarias, en línea, a través de Suntrust.com. Nuestros archivos indican que recientemente reprogramó su clave. Este aviso es para confirmarle que usted hizo este cambio. Si cree haber recibido este correo electrónico por equivocación y no reprogramó su clave, por favor haga clic aquí.

Atentamente,
David H. Stone
Director de Apoyo a Clientes
Suntrust Corporation – eCommerce Division

Business Banking | Corporate & Institutional

SUNTRUST Personal Finance

E-MAIL CHANGE NOTIFICATION

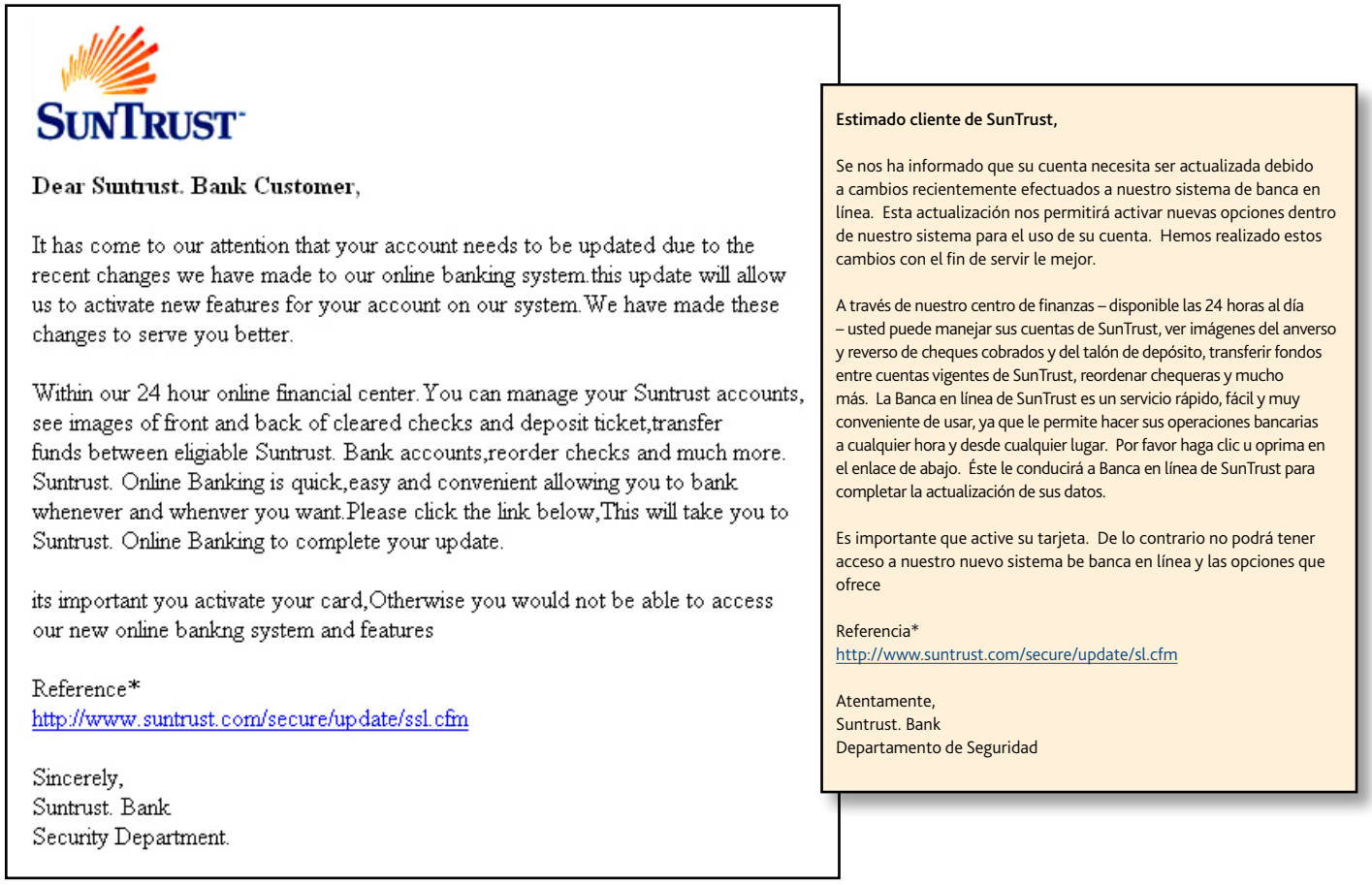
Dear [redacted]

Thank you for banking online at suntrust.com. Our records indicate that you recently reset your password. This notification is to confirm that you initiated this change.
If you feel you have received this email in error and did not reset you password, please click here
Sincerely,
David H. Stone
Director of Customer Advocacy
Suntrust Corporation - eCommerce Division

Suntrust Bank, N.A. Member FDIC

Contact Us
(800) 654-1276
24 hours a day
seven days a week
electronic.services@suntrust.com

Éste es el ejemplo de una página web falsa o fraudulenta:



SUNTRUST

Dear Suntrust. Bank Customer,

It has come to our attention that your account needs to be updated due to the recent changes we have made to our online banking system.this update will allow us to activate new features for your account on our system.We have made these changes to serve you better.

Within our 24 hour online financial center.You can manage your Suntrust accounts, see images of front and back of cleared checks and deposit ticket,transfer funds between eligiable Suntrust. Bank accounts,reorder checks and much more. Suntrust. Online Banking is quick,easy and convenient allowing you to bank whenever and whenver you want.Please click the link below,This will take you to Suntrust. Online Banking to complete your update.

its important you activate your card,Otherwise you would not be able to access our new online bankng system and features

Reference*
http://www.suntrust.com/secure/update/ssl.cfm

Sincerely,
Suntrust. Bank
Security Department.

Estimado cliente de SunTrust,

Se nos ha informado que su cuenta necesita ser actualizada debido a cambios recientemente efectuados a nuestro sistema de banca en línea. Esta actualización nos permitirá activar nuevas opciones dentro de nuestro sistema para el uso de su cuenta. Hemos realizado estos cambios con el fin de servir le mejor.

A través de nuestro centro de finanzas – disponible las 24 horas al día – usted puede manejar sus cuentas de SunTrust, ver imágenes del anverso y reverso de cheques cobrados y del talón de depósito, transferir fondos entre cuentas vigentes de SunTrust, reordenar chequeras y mucho más. La Banca en línea de SunTrust es un servicio rápido, fácil y muy conveniente de usar, ya que le permite hacer sus operaciones bancarias a cualquier hora y desde cualquier lugar. Por favor haga clic u oprima en el enlace de abajo. Éste le conducirá a Banca en línea de SunTrust para completar la actualización de sus datos.

Es importante que active su tarjeta. De lo contrario no podrá tener acceso a nuestro nuevo sistema be banca en línea y las opciones que ofrece

Referencia*
http://www.suntrust.com/secure/update/sl.cfm

Atentamente,
Suntrust. Bank
Departamento de Seguridad

Este sitio web fraudulento tiene exactamente la misma apariencia que la página inicial de SunTrust Bank, pero los caracteres del URL o dirección no son https://www.suntrust.com.

¿Cómo obtienen los ladrones de identidad su dirección de correo electrónico?
Los ladrones de identidad envían al azar correos electrónicos fraudulentos que parecen provenir de un banco con el que usted podría tener o no tener una cuenta. También recopilan información personal y sobre las cuentas a través de virus incrustados en los correos electrónicos, o pueden comprar legítimamente listas de envío postal y obtener correos electrónicos de Internet a través de sitios web, salas de chateo, subastas en línea o directorios.

Nuestra política de confidencialidad estipula que SunTrust no comercia, alquila ni vende la información personal de su clientela, incluyendo las direcciones de correo electrónico.

Ayude a prevenir el fraude en línea

Usted puede salvaguardar su identidad y sus cuentas de muchas maneras. A continuación le proporcionamos una serie de sugerencias para hacerlo:

- **No ponga atención sólo en el logotipo.** Con el fin de lograr que los mensajes de correos electrónicos o sitios web parezcan ser legítimos, los ladrones de identidad con frecuencia incluyen logotipos e imágenes reales de compañías auténticas. También procuran transmitir un sentido de urgencia afirmando que si no proporciona, actualiza o verifica su información personal o sobre sus cuentas se suspenderá su acceso a las mismas. Haga caso omiso de estos sitios web aparentemente legítimos y no proporcione ningún tipo de información.
- **Utilice un filtro de "spam", es decir, publicidad no deseada.** Muchos servicios de correo electrónico ahora ofrecen filtros de "spam" que minimizan la cantidad de correos electrónicos no solicitados que usted recibe. Estos filtros pueden ayudar a reducir los correos electrónicos fraudulentos que usted pudiera recibir.
- **Escriba, no haga clic.** Si llegara a abrir un correo electrónico sospechoso, no haga clic en ningún vínculo ya que, sin darse cuenta, podría pasarle un virus a su computadora o descargar software espía. Incluso si cree que el correo electrónico es legítimo, escriba la dirección del sitio web en la ventana de su programa de navegación en lugar de utilizar el vínculo. Si el mensaje proviene de una institución con la que usted tiene una relación comercial, utilice la lista de favoritos que ya creó al visitar el sitio web auténtico de la compañía.
- **Cambie las contraseñas que usa en Internet cada 30 a 60 días**. Sea creativo con sus contraseñas – evite lo obvio como su código postal, su fecha de nacimiento o información delicada como el nombre de soltera de su madre o su número del Seguro Social.
- **Actualice su software anti-virus y anti-"spam"**. Al tener al día el software anti-virus y anti-"spam" de su computadora, hace más difícil que los delincuentes puedan obtener acceso a su información personal y a la información de sus cuentas. La mayoría de los proveedores de programas anti-virus y anti-"spam" ofrecen servicios de suscripción a fin de garantizar que usted reciba todas las más recientes actualizaciones del software. Si no está seguro si su software está actualizado, comuníquese con su prestador de servicios anti-virus o anti-"spam".

¿Cómo salvaguarda SunTrust la información de su clientela?

Estamos comprometidos con mantener la información de nuestros clientes a salvo del acceso no autorizado y de conservar la confidencialidad de sus identidades. En nuestro sitio web, hacemos uso de toda la tecnología estándar en el sector, tal como encriptación, "firewalls" y contraseñas.

En SunTrust, hemos implantado estrictas políticas de privacidad y confidencialidad. SunTrust no comercia, alquila ni vende la información personal de su clientela, incluyendo las direcciones de correo electrónico. No proporcionamos información personal ni información sobre las cuentas a compañías que no forman parte de la familia SunTrust para fines de telemercadeo independiente o promociones postales de productos o servicios no financieros. Si desea obtener información adicional sobre nuestra política de confidencialidad y privacidad, visite suntrust.com/privacy.

Compromiso de SunTrust con los clientes

SunTrust jamás enviará mensajes electrónicos pidiéndole a los clientes que suministren, actualicen o comprueben la información personal ni de la cuenta, tal como contraseñas, números del Seguro Social, números de identificación personal, los números de la tarjeta de débito, o alguna otra información confidencial.

¿Cómo reportar el fraude en línea en relación con su cuenta de SunTrust?

- Si desea informar un mensaje de correo electrónico o página web sospechoso, re-envíelo a reportfraud@suntrust.com.
- Si proporcionó información personal o sobre su cuenta en lo que, en su opinión, podría ser un correo electrónico o sitio web fraudulento, comuníquese de inmediato con uno de los representantes de SunTrust llamando al 800.227.3782 o visite suntrust.com/alert y llene el Formulario de fraude en línea (Online Fraud Form).

Su mejor protección contra el robo de identidad y el fraude en línea es usted mismo. Al mantenerse informado y ejercer precaución al divulgar su información confidencial, podrá ayudar a proteger tanto su identidad como sus cuentas. Si desea obtener información adicional sobre el fraude en línea, visite suntrust.com/alert.

En caso de convertirse en víctima del robo de identidad...

Si cree que fue víctima del robo de identidad, tome las siguientes medidas de inmediato:

- **Notificar a una de las tres principales compañías de elaboración de informes de crédito y colocar una advertencia de fraude en su informe de crédito.** Llame al número gratuito de cualquiera de las tres principales compañías de informes de crédito para notificar fraudes a fin de que coloquen una advertencia de fraude en su informe de crédito. Esto podría ayudar a evitar que el ladrón pueda abrir cuentas adicionales a nombre de usted. Una vez que la compañía de informes de crédito confirme que ha colocado su advertencia de fraude, las otras dos compañías de crédito serán notificadas automáticamente.
- **Comuníquese con sus instituciones financieras y con las compañías emisoras de sus tarjetas de crédito**. Cierre las cuentas que exhiban retiros o cargos no autorizados y abra nuevas cuentas con nuevos números de identificación personal (PIN) y contraseñas.
- **Notifique al departamento de policía de su localidad**. Incluso si la policía no atrapa al criminal, presentar un informe policíaco puede ayudarlo a enmendar su informe de crédito. Pida el número de caso y una copia de su informe.
- **Comuníquese con todos los negocios en donde se han abierto cuentas a su nombre sin su autorización.** Cierre las cuentas e informe a las empresas que las cuentas fueron abiertas de manera fraudulenta. Asegúrese de comunicarse con los negocios por escrito.
- **Notifique a la FTC (Federal Trade Commission o Comisión federal de comercio)** llamando al 877.ID.THEFT (877.438.4338) o visite consumer.gov/idtheft. Al compartir su denuncia de robo de identidad con la FTC, estará proporcionando importante información que podría ayudar a los oficiales policíacos a identificar ladrones de identidad.
- **Reporte la correspondencia robada**. Presente un informe ante el Servicio Postal. Llame al inspector postal de su localidad o visite usps.com.
- **Reporte su número de Seguro Social como robado.** Llame a la Línea Directa de Fraudes del Seguro Social al 800.269.0271.
- **Reporte los cheques robados**. Si le robaron cheques o sus cheques han sido utilizados indebidamente, cierre todas las cuentas afectadas y comuníquese con las siguientes compañías de verificación de cheques:

  TeleCheck 800.710.9898

  Certegy 800.437.5120

- **Notifique a la SEC (Securities and Exchange Commission o Comisión de acciones y valores) llamando al 800.732.0330**. Si identifica actividades sospechosas en sus cuentas de inversiones, comuníquese de inmediato con la SEC.

Esta guía incluye una hoja de trabajo cuyo objetivo es ayudarle a documentar las notificaciones de robo de identidad a las compañías de informes de crédito, oficiales policíacos, negocios e instituciones financieras.

Muestra de cartas de disputa

Si usted llegara a convertirse en víctima del robo de identidad, puede usar las siguientes cartas de muestra para disputar los cargos realizados indebidamente en sus cuentas. Todas las comunicaciones deberán realizarse por escrito y debe sacar copias de toda su correspondencia a fin de conservarla en sus archivos.

Muestra de carta de disputa dirigida a las compañías de informes de crédito*

Fecha

Su nombre
Su dirección
Su ciudad, estado, código postal

Departamento de quejas
Nombre de la compañía de informes de crédito
Dirección
Su ciudad, estado, código postal

Estimado(a): _____

El motivo de la presente carta es disputar la siguiente información en mi expediente. La información en disputa también se encuentra encerrada en un círculo en la copia adjunta del informe que recibí. (Identifique el nombre de la fuente del[de los] cargo[s] dipitado[s] tales como acreedores o tribunal fiscal, e identifique el tipo de cargo, tal como cuenta de crédito, disposición del juez, etc.)

Soy víctima del robo de mi identidad y no he efectuado el(los) cargo(s). Por ello, me permito solicitar que el cargo sea bloqueado a fin de corregir mi informe de crédito.

Adjunto a la presente sírvanse encontrar copias de (use esta frase si se aplica a su caso y describa la documentación adjunta) a fin de dar apoyo a mi posición. Por favor, le ruego se investigue este asunto y bloquear el(los) cargo(s) disputados a la mayor brevedad posible.

Atentamente,

Su nombre

Anexos: (lista de los documentos que adjunta)

*Fuente: FTC en ftc.gov/bcp/conline/pubs/credit/idtheft.htm

Muestra de carta de disputa para cuentas de crédito preexistentes*

Fecha

Su nombre
Su dirección
Su ciudad, estado, código postal
Su número de cuenta

Nombre del acreedor
Información de facturación
Dirección
Su ciudad, estado, código postal

Estimado(a): _____

El motivo de la presente carta es disputar un (cargo o débito) fraudulento atribuido a mi cuenta por la cantidad de $_____. Soy víctima del robo de mi identidad y yo no efectué este (cargo o débito). A través de la presente le solicito se sirva (eliminar el cargo o restituir el débito), que todos los cargos relacionados con la cantidad fraudulenta sean acreditados, incluyendo los cargos por concepto de financiamiento, y que yo reciba un estado de cuenta correcto.

Adjunto copias de (use esta frase para describir cualquier información adjunta, tal como un informe policíaco) como apoyo a mi posición. Por favor, le ruego se sirvan investigar este asunto y corregir el (cargo o débito) fraudulento a la mayor brevedad posible.

Atentamente,

Su nombre

Anexos: (lista de los documentos que adjunta)

*Fuente: FTC en ftc.gov/bcp/conline/pubs/credit/idtheft.htm

Obtenga información adicional sobre el fraude y el robo de identidad en línea

La mejor forma de protegerse contra el robo de identidad y el fraude en línea es tener precaución al proporcionar información personal y sobre sus cuentas, así como mantenerse informado sobre ese tipo de engaños. Por favor, visite estos vínculos a fin de obtener información adicional:

- SunTrust: suntrust.com/alert
- FTC (consumidor): consumer.gov/idtheft
- Inspectores del USPS: usps.gov/postalinspectors
- FTC (spam): ftc.gov/spam

Compañías de informes de crédito
Informe el fraude a por lo menos una de las compañías de informes de crédito y solicite una copia de su informe de crédito.

Compañía	Número telefónico	Fecha de contacto	Persona contactada	Comentarios
Equifax	800.525.6285			
TransUnion	800.680.7289			
Experian	800.397.3742			

Autoridades policíacas – Informe el robo de identidad

Agencia	Número telefónico	Fecha de contacto	Persona contactada	Comentarios
Departamento de Policía local				
Comisión federal de comercio	877.438.4338 o ftc.gov			
Administración del Seguro Social	800.269.0271			
Servicio Postal de los EE.UU.	Oficina postal local			

Bancos, emisores de tarjetas de crédito y otros acreedores

Acreedor	Dirección y número telefónico	Fecha de contacto	Persona contactada	Comentarios
Grupo de servicios sobre el robo de identidad de SunTrust	866.493.3446, opción 2			