

# Información Importante Sobre el Robo de Identidad de Regions

Cómo usted se puede proteger del robo de identidad y qué puede hacer si piensa que es una víctima.



© 2011 Regions Bank. Member FDIC.

# Índice

- Introducción ..... 2
- ¿Qué es el Robo de Identidad? ..... 3
- Como Funciona el Robo de Identidad ..... 3
- Lo que Puede Hacer para Proteger su Identidad ..... 7
- Lo que Está Haciendo Regions para Proteger su Identidad ..... 14
- A Quien Puede Contactar si Usted es o Podría ser una Víctima de Robo de Identidad ..... 16
- Como Debería Manejar sus Cuentas de Regions ..... 17
- Identity Theft Assistance Corporation (ITAC) ..... 18
- Acuerdo y Descripción de Servicios de ITAC ..... 19
- Afidávit Estándar para Robo de Identidad ..... 20
- Registro de Acción Contra Robo de Identidad de Regions ..... 24

## En Regions, el servicio al cliente es importante.

Nosotros valoramos las relaciones con nuestros clientes y sus familias y esperamos que usted nunca sea víctima de robo de identidad. Pero como las incidencias de robo de identidad están aumentando, nosotros queremos que usted esté al tanto de las precauciones más básicas que debe tomar para protegerse de este crimen. Hemos creado el Paquete de Robo de Identidad de Regions para ayudarle a entender el crimen y minimizar el riesgo. Aquí estamos incluyendo medidas de seguridad y sugerencias para resguardar su información personal, hacer transacciones financieras por Internet, navegar el Internet de una manera segura y proteger su identidad por Internet.

Además de proveerle información sobre como proteger su identidad, también hemos incluido una lista de contactos e información importante con respecto a qué debe hacer si sospecha que ha sido una víctima de robo de identidad. También le hemos proveído un Registro de Acción Contra Robo de Identidad para ayudarle a documentar los pasos que puede tener que tomar.

Para más información sobre el fraude y robo de identidad, además de maneras de como protegerse de estos crímenes, por favor visite la sección de Privacidad y Seguridad en [regions.com/espanol](https://regions.com/espanol).

## ¿Qué es el Robo de Identidad?

El robo de identidad ocurre cuando un criminal usa su información personal — como su nombre, dirección y Número de Seguro Social — y lo usa para establecer crédito y comprar cosas a su nombre. Para cometer robo de identidad, los pillos pueden robarse la información necesaria de ciertas maneras:

- Usando cuentas o estados de cuenta que ha botado
- Usando una billetera perdida
- Usando correspondencia personal robada
- Obteniendo una copia de su reporte de crédito
- A través de actividades fraudulentas por Internet, teléfono o mensajes de texto
- Usando información que usted ha divulgado por Internet

## Como Funciona el Robo de Identidad

Los criminales pueden robar su identidad usando una variedad de técnicas. Algunas de las técnicas son las siguientes:

### Phishing

“Phishing” es una manera de piratería por Internet donde los maliciosos están tratando de “pescar” su información financiera personal. Ellos quieren sus números de cuenta, contraseñas, Números de Seguro Social y otra información confidencial que pueden usar para saquear su cuenta de cheques o comprar cosas con sus tarjetas de crédito. En un caso típico, usted recibirá un email que aparenta venir de una compañía reconocida con la que usted hace negocios, como por ejemplo, su institución financiera. En algunos casos, el email puede aparentar ser de una agencia del gobierno, incluyendo agencias federales que regulan instituciones financieras. El email probablemente le advertirá que hay un problema serio que requiere su atención inmediata. Puede usar frases como “Requiere su atención inmediata”, o “Por favor contáctenos inmediatamente con respecto a su cuenta”. El email le pedirá que responda o que haga clic en un botón para ir a la página de Internet de la institución. En una estafa de “phishing”, usted podrá ser llevado a una página de Internet que puede lucir exactamente como la página verdadera.

De hecho, a veces puede ser la página verdadera de la compañía. En esos casos, una ventana adicional aparecerá con el propósito de robarse su información financiera.

En estos casos le pueden pedir que actualice su información personal o que provea su información para verificación: su Número de Seguro Social, número de cuenta, contraseña, Número de Identificación Personal (PIN) o la información que usted usa para verificar su identidad cuando está hablando con una institución financiera verdadera, como el apellido de soltera de su mamá, su fecha o lugar de nacimiento o contestaciones a preguntas de seguridad.

Si provee la información que le han pedido, usted puede ser la víctima de robo de identidad. Recuerde, **REGIONS NUNCA LE PEDIRÁ ESTA INFORMACIÓN POR EMAIL.**

**Por favor mándenos cualquier email sospechoso a [phishing@regions.com](mailto:phishing@regions.com).** También le recomendamos que no abra ningún programa (por ejemplo, archivos con extensión .exe) o archivos .zip a no ser que sea de una persona o institución en la que usted confía.

## “Vishing” y “Smishing”

Variaciones de “phishing” incluyen “vishing” y “smishing”. “Vishing” es cuando usted recibe un email, supuestamente de parte de un remitente conocido, pidiéndole que llame a un número de teléfono urgentemente. Luego le pedirán que provea información confidencial. Ataques de “smishing” usan mensajes de texto — de nuevo, aparentando ser de un remitente legítimo y con un mensaje urgente — pidiéndole que haga clic en el enlace de un mensaje y luego que provea información confidencial.

## Protección de Robo de Identidad Falsa o Estafa de Reparación de Crédito

Estafas de reparación de crédito le ofrecen borrar información negativa de su archivo de crédito para que pueda calificar para una tarjeta de crédito, préstamo de auto, hipoteca de casa o un trabajo. El Federal Trade Commission (FTC), la agencia que, entre otras cosas, se encarga de proteger a los consumidores, ha advertido que algunas compañías dicen que proveen servicios de prevención de robo de identidad, pero que de hecho son

personas tratando de robarle su número de licencia de conducir, el apellido de soltera de su mamá, Número de Seguro Social y números de cuenta de banco y tarjeta de crédito. El FTC le ha advertido a los consumidores que no divulguen ninguna información personal por teléfono o por Internet a no ser que esté familiarizado con la compañía que se la está pidiendo. Si no está seguro de una compañía, verifíquela con el Better Business Bureau antes de divulgar cualquier información que le están pidiendo. Las personas que promueven estos servicios fraudulentos no pueden hacer nada para ayudar a reparar su crédito. Está al tanto de que pueden recomendar que usted mienta en una solicitud de préstamo o crédito, falsifique su Número de Seguro Social o que obtenga un Número de Identificación de Empleador bajo pretextos falsos — todas situaciones donde usted estaría violando la ley federal.

## Estafa de “Tiene Que Actualizar Su Cuenta”

Este tipo de fraude usualmente aparece en su email con un mensaje del “Administrador de Sistema” diciéndole que tiene que darle mantenimiento urgente a su cuenta o que debe verificar su información de cuenta y Número de Seguro Social. Si este tipo de email tiene un enlace, no le haga clic.

## Estafa Especial de Visa®/MasterCard®

Este fraude conlleva una llamada telefónica de un “empleado” de Visa o MasterCard que está tratando de confirmar unos gastos inusuales. Luego le pedirán el “Código de Seguridad” de tres dígitos en la parte de atrás de su tarjeta de crédito. Nunca debería darle a nadie el código en la parte de atrás de su tarjeta de crédito a no ser que usted inició la llamada a un comerciante reconocido. Si no está seguro, enganche el teléfono y llame al número de fraude en la parte de atrás de su tarjeta de crédito.

## Estafa de “Reporte de Crédito Gratis”

Casi todos los emails que recibe con respecto a “reportes de crédito gratis” son fraudulentos. La persona está tratando de averiguar su Número de Seguro Social o le está mandando una cuenta por proveerle un servicio. Investigue la compañía a través del Better Business Bureau y el FTC.

Si provee la información que le han pedido, usted puede ser la víctima de robo de identidad. Recuerde, REGIONS NUNCA LE PEDIRÁ ESTA INFORMACIÓN POR EMAIL.

## Rebuscando la Basura

Aunque no lo crea, hay criminales que rebuscan la basura de negocios o casas buscando información confidencial de consumidores. Ellos también pueden rebuscar los recipientes comunales buscando récords, correspondencia u otros papeles que la gente haya botado. Triture cualquier documento que tenga información confidencial.

## Robando Buzones

Los criminales robarán correspondencia de los buzones, sea correspondencia que usted mandó o que recibirá. Estos criminales están buscando cuentas de tarjetas de crédito, estados de cuentas de banco, ofertas de tarjetas de crédito y otra correspondencia que puede tener información personal que lo identifique.

## Robando Billeteras, Carteras u Otros Artículos

Los criminales no sólo tienden a usar billeteras perdidas o robadas para usar las tarjetas de crédito robadas, si no también para establecer crédito adicional a nombre del dueño. Muchas veces, si hay cheques entre los artículos robados, el pillo visitará el banco de la víctima pretendiendo ser un cliente y tratando de cambiar los cheques.

## Estafa de Nigeria

Aunque no es un tipo de robo de identidad verdadero, la estafa de Nigeria está en pie desde hace mucho tiempo y le ha causado mucho daño a sus víctimas. Este tipo de fraude conlleva cartas y emails no solicitados que les mandan a individuos y compañías ofreciéndole al destinatario algo valioso por ayudarles a transferir millones de dólares a bancos americanos. Otros tipos de “fraudes tradicionales” incluyen oportunidades de negocios falsas, cartas de secuencia, “artículos gratis”, estafas de trabajar en la casa, fraudes de dietas, etc.

## Lo que Puede Hacer para Proteger su Identidad

Puede tomar ciertos pasos para protegerse usted mismo y su identidad. Más adelante hay unas advertencias, incluyendo como debe protegerse mientras navega el Internet:

- **Estados de Cuenta Bancarios y de Crédito**

Revise sus estados de cuenta bancarios y de crédito con tiempo y reporte cualquier discrepancia o transacciones sospechosas inmediatamente. También, reporte cualquier discrepancia que usted vea mientras esté haciendo otras transacciones de rutina (o sea, transacciones de ATM, por Internet, etc.). Reporte cheques, tarjetas de crédito y tarjetas de cheques/ATM perdidas o robadas tan pronto descubra que las ha perdido.

- **Monitoree su Reporte de Crédito**

Monitoree su reporte de crédito anualmente para consultas y cuentas desconocidas. Usted tiene el derecho de recibir una divulgación gratis de su archivo de crédito cada 12 meses de cada una de las agencias nacionales que reportan el crédito de los consumidores — Equifax, Experian y TransUnion. Este archivo de crédito gratis se puede pedir en [annualcreditreport.com](http://annualcreditreport.com) o llamando al 877-322-8228. Usted tiene la opción de pedir los 3 a la misma vez (el cual le permite comparar los datos de las 3 compañías), o puede ordenar uno de cada una de las agencias en intervalos periódicos (el cual le puede alertar de cualquier cambio en su reporte de crédito).

También hemos encontrado una manera fácil y segura para que usted se mantenga al tanto de su crédito y ayude a protegerse del robo de identidad. Es un sistema de advertencia temprana llamado **IdentityProtect<sup>SM</sup> de Regions** — y es uno de los únicos programas de protección completa que le ayuda a monitorear su crédito no sólo una vez al año, pero diariamente. (Lea la página 11 para detalles.)

- **Tome Precauciones con su Correspondencia**

Acostúmbrese a colocar su correspondencia saliente que contenga pagos o información confidencial en un buzón del Correo o en la oficina del Correo más cercana. Si va a estar de viaje o no podrá recoger su correspondencia, pídale a un amigo que la recoja o pídale al Correo que se quede con ella temporariamente. Para asegurarse que su

estado de cuenta esté seguro, considere recibirlo en un formato electrónico. Puede inscribirse en Banca por Internet de Regions con estados de cuenta electrónicos en [www.regions.com/espanol](http://www.regions.com/espanol).

- **Tome Precauciones con su Basura**

Considere comprar una trituradora. No cometa el error de botar descuidadamente los estados de tarjetas de crédito con cheques de cortesía adjuntos, ofertas de tarjetas de crédito, correspondencia o cualquier otro papeleo que pueda tener información personal. Triture estos artículos o rómpalos cuidadosamente para que los pillos no puedan rebuscar su basura y robarse su información confidencial.

- **Sepa Quien lo Está Llamando**

Recuerde que los ladrones de identidad pueden usar muchos trucos y engaños para obtener información por teléfono. Ellos pueden pretender ser alguien de su banco, cooperativa de crédito, compañía de servicios u otra compañía con la que usted hace negocios frecuentemente. A no ser que usted inició la llamada, no le dé ninguna información personal por teléfono a alguien que no conoce.

- **Resguarde su Información Personal**

Su Número de Seguro Social, números de tarjetas de crédito y otra información confidencial es exactamente lo que buscan los ladrones de identidad. Use buen juicio cuando tenga esa información con usted. Por ejemplo, usted por lo general no tiene que estar cargando con su Tarjeta de Seguro Social, y puede que sólo necesite tener una tarjeta de crédito en vez de muchas tarjetas. Considere almacenar la información que no le hace falta en un lugar seguro en su casa o en una caja de seguridad en vez de su billetera o cartera.

- **Nombres de Usuario y Contraseñas por Internet**

Nunca provea por teléfono sus contraseñas de cuentas por Internet ni responda a un pedido no solicitado por Internet o email. Regions nunca le pedirá que verifique su información de cuenta por email, ni lo llamaremos para pedirle su contraseña de cuenta por Internet. Nombres de usuario y contraseñas de cuentas por Internet son

extremadamente confidenciales y nunca se las debería dar a nadie. Asegúrese que escoja nombres y contraseñas que usted recuerde fácilmente pero que otras personas prácticamente no puedan averiguar, y nunca escriba su contraseña en un papel. No use los últimos cuatro dígitos de su Número de Seguro Social o cualquier otra información personal para su nombre de usuario o contraseña. Cambie su contraseña cada mes o dos meses. Si alguien ha averiguado su contraseña, cámbiela inmediatamente.

- **Preguntas de Seguridad de Banca por Internet**

Si usted usa la Banca por Internet de Regions, no le dé las contestaciones de sus preguntas de seguridad a nadie. Estas preguntas están diseñadas para proteger sus cuentas de acceso no autorizado. Le podemos hacer una de estas preguntas si nuestro sistema detecta que trató de ingresar a su cuenta de una manera inusual.

- **Divulgar su Información Personal por Internet**

Mientras usted navega el Internet y encuentra páginas que disfruta, le pueden pedir que llene formularios y dé su información personal. Asegúrese que esté al tanto de la política de privacidad de la compañía. Si usted no opta para que no divulguen su información, ellos pueden vender o compartir su información con un tercero. Recuerde, Regions nunca lo llamará por teléfono ni le mandará un email para pedirle o para que usted verifique su Número de Cliente de Banca por Internet, PIN o cualquier otra información confidencial. Sin embargo, si usted contacta al banco, nosotros le pediremos información que nos permita verificar su identidad para poder proteger su privacidad.

- **Monitoreando sus “Cookies”**

“Cookies” son archivos pequeños que las páginas de Internet colocan en el disco duro de su computadora y que buscan la próxima vez que usted visite su página. En las páginas que usted visita frecuentemente, estos archivos se mantienen al tanto de lo que usted ha hecho ahí antes y tratan de hacer sus preferencias más automatizadas. Monitoree todas sus transacciones con estos archivos configurando las preferencias de seguridad de su navegador para que le pregunte si quiere aceptar cualquier “cookie”.

- **Ir de Compras por Internet**

Conozca al comerciante. Sólo le compre a aquellas compañías con las que usted se siente cómodo o a aquellas que toman pasos adicionales para comunicarle sus intenciones honestas a través de una política transparente y sellos de organizaciones de protección del consumidor. El FTC mantiene una página de Internet — [consumer.gov](http://consumer.gov) — la cual incluye guías, sugerencias y enlaces a recursos para consumidores.

Use una tarjeta de crédito. Pagar con tarjetas de crédito es un buen hábito, porque bajo ley federal (y su acuerdo de tarjeta de crédito) su responsabilidad por un cargo no autorizado está limitado a \$50. Cuando use su tarjeta de crédito por Internet, no dé su número de tarjeta a no ser que esté entrando en una página que codifique su número. Debería poder ver el “https” en la dirección de la página, y el símbolo del candado también debería aparecer en su pantalla.

- **Banca por Internet**

Las páginas de Internet de los bancos usualmente están divididas en dos secciones: la página de Internet pública a la que cualquiera tiene acceso y la página segura que requiere una combinación de identificación y contraseñas a la cual sólo los clientes del banco tienen acceso. Como mencionamos en la sección de Navegadores, si usted está viendo o enviando información privada, busque conexiones seguras o codificadas — aquellas con “https” en su dirección o con un icono de un candado cerrado. También, asegúrese de no comunicar ninguna información personal a través de la página de un banco a no ser que esté usando una conexión segura. Si no hace esto, corre el riesgo que otra persona se robe esta información. Antes de ir a la próxima página, asegúrese de terminar su sesión de banca por Internet saliendo de su cuenta. Si no sale de su cuenta, su sesión de banca por Internet continuará hasta que pare automáticamente, lo cual puede tomar varios minutos. En muchas ocasiones, si usted va a otra página sin salir de su cuenta, su información bancaria todavía se puede encontrar con sólo hacerle clic al botón de Regresar del navegador.

- **Pagando Cuentas por Internet**

Sólo debería pagar sus cuentas a través de una conexión de Internet segura. Mientras proteja la identidad de su nombre de usuario y contraseñas de banca por Internet, el pago de cuentas por Internet estará seguro.

- **Navegue el Internet de una Manera Segura**

Los navegadores sólo son programas que su computadora usa para comunicarse con servidores de Internet y páginas de Internet de demostración. Información a la que usted tiene acceso en las páginas de Internet viaja entre su computadora y un servidor de Internet a través de una serie de computadoras y usted no sabe qué computadoras estarán manejando su información. Por lo tanto, se han creado ciertos mecanismos de protección que aseguran la transmisión de sus datos confidenciales. La codificación — el proceso de transformar datos a un formato que sólo pueden leer los que tienen la “llave” para decodificarlo — es una manera de resguardar su información cuando se transmite por Internet.

— **¿Cómo funciona la codificación?**

Antes de que su computadora envíe la información, se codifica usando una “llave” especial que convierte la información a un formato ilegible. Mientras esta información codificada atraviesa el Internet, es extremadamente difícil e impráctico tratar de descifrarla. Tan pronto llega a su último destino, se decodifica usando otra “llave” especial y se convierte a un formato que se puede usar.

— **¿Cómo mantengo actualizada la seguridad de mi navegador?**

Asegúrese que siempre esté usando el navegador más actualizado y seguro disponible para aprovechar de los programas más recientes que lo protegen de virus, gusanos y otros programas maliciosos que existen en el Internet. Hay dos tipos de navegadores seguros actualmente disponibles: con codificación de 40 bytes y codificación de 128 bytes. Regions requiere una codificación de 128 bytes, la cual es la más segura. Muchos expertos en seguridad recomiendan actualizar su navegador de Internet a la versión más reciente.

- **Más Sugerencias para Navegadores**

- Nunca abra más de un navegador o visite otra página de Internet que no sea segura mientras está llevando a cabo una transacción segura por Internet.
- Siempre cierre y abra de nuevo su navegador antes y después de una sesión segura.
- Apague los “comportamientos de secuencia de comandos” en su navegador. Algunas páginas de Internet no abrirán si estos comandos no están funcionando y puede tener problema con su servicio de correo por Internet. Si ese es el caso, tendrá que establecer unas direcciones de Internet para que funcionen de nuevo. Consulte el manual de su computadora para direcciones o contacte a la compañía para que le ayude con este proceso.
- Establezca firewalls de software y hardware en su computadora. Los programas de firewalls de software son relativamente económicos.
- Desconéctese del Internet cuando no lo esté usando activamente. Dejar su conexión de Internet abierta es como dejar su puerta abierta toda la noche. Si deja su Internet abierto, cualquier cosa puede entrar en cualquier momento. Y nuevamente, termine su sesión.
- Si está navegando una página de Internet de Regions y recibe una advertencia de un certificado de seguridad inválido, esto puede indicar que tiene una infección maliciosa en su computadora. Favor llame inmediatamente al Servicio al Cliente de Banca por Internet al 1-800-472-2265.

- **Spyware de Control**

Spyware es un programa escondido que se instala en una computadora sin el consentimiento del dueño con el propósito de recolectar datos personales secretamente. Anunciantes y piratas informáticos luego pueden usar esta información. Spyware puede monitorear pulsación de teclas, contraseñas, números de tarjetas de crédito,

páginas de Internet que visita y mucho más. Básicamente cualquier cosa en su computadora está disponible para los pillos a no ser que usted se proteja. Es bien común que los programas de spyware estén mal hechos y en muchos casos tienen problemas que causan fallos en su computadora como apagones inesperados o causan que su rendimiento empeore tremendamente. Una manera de proteger su computadora es desinstalando programas que ya no está usando. Esto es un buen hábito y le permitirá encontrar cualquier programa nuevo que fue instalado sin su autorización.

Otra manera de tomar la iniciativa es siempre evaluando la política de privacidad de la compañía y el acuerdo de licencia antes de instalar cualquier programa. Las compañías de spyware se aseguran de esconder sus intenciones y es igual de importante saber como las compañías legítimas piensan usar la información que ellos recolectan. También es importante que sepa que instalar programas antivirus no protegen a su computadora de cualquier tipo de spyware. Utilizar programas anti-spyware especiales es la mejor manera de protegerse. Además, los programas anti-malware lo pueden proteger de una variedad de códigos maliciosos que típicamente incluyen virus y spyware.

- **IdentityProtect de Regions**

Para ayudarle a proteger su identidad, a lo mejor quiere considerar inscribirse en IdentityProtect de Regions. Por sólo \$5 al mes, el IdentityProtect de Regions resguarda su identidad con:

- Alerta a las Tres Agencias de Crédito para notificarle de cualquier cambio a su crédito.
- Card Patrol<sup>SM</sup>, una herramienta por Internet especial administrada por expertos en seguridad que busca todos los números de sus tarjetas de crédito o débito registradas que podrían haber sido robados.
- Elegibilidad para Seguro de Robo de Identidad.\*

El IdentityProtect de Regions está incluido con ciertos productos de cuentas de cheques a ningún costo adicional. Hable con un representante de Regions para detalles.

*\*El Seguro de Robo de Identidad está proveído por Chartis, Inc. Productos de seguro no están asegurados por el FDIC, no son un depósito, no son una obligación ni están garantizados por Regions Financial Corporation, sus filiales, ni cualquier agencia del gobierno.*

## Lo que Está Haciendo Regions para Proteger su Identidad

Regions sigue unos procedimientos estrictos de seguridad de información diseñados para proteger la confidencialidad de su información. También usamos la tecnología más reciente para asegurar la confidencialidad de sus datos bancarios. Adelantos en la tecnología de seguridad ocurren frecuentemente, y Regions continua evaluando nuestro ambiente de seguridad para asegurarse que está proveyéndole a nuestros consumidores el nivel de privacidad y seguridad más alto. Nuestra primera prioridad es proteger y asegurar las transacciones financieras y los sistemas en las que dependen esas transacciones.

### Seguridad de Cuentas General


- Regions monitorea actividad de cheques, tarjetas de débito, transferencias bancarias y ACH (pagos electrónicos) para buscar cualquier actividad sospechosa en sus cuentas.
- Además de ofrecer servicios de ITAC (lea la página 15), la Seguridad Corporativa de Regions le ayudará a contactar otros bancos para hacer cualquier reclamación necesaria si usted piensa que ha sido la víctima de robo de identidad.

### La Seguridad de Banca por Internet de Regions

- Los productos por Internet de Regions usan la tecnología de codificación más reciente para asegurar sus datos por Internet. La codificación es el proceso de transformar datos a un formato que sólo pueden leer los que tienen la “llave” para decodificarlo.
- Para su protección, Regions usa codificación de 128 bytes a través de la página de Banca por Internet de Regions. Si su navegador no puede manejar codificación de 128 bytes, usted puede descargar un navegador nuevo gratis.
- Regions usa autenticación de varios factores para proteger sus cuentas a través de Banca por Internet. Si nuestro sistema detecta un intento de ingreso a su cuenta que no es normal, le pediremos que conteste una de las preguntas de seguridad que ya usted estableció.

- Regions usa certificados digitales para asegurarse que cuando usted entre en nuestras páginas aseguradas, usted está comunicándose con Regions y no con un impostor.
- Si recibe un email pidiéndole que ingrese en su cuenta de Banca por Internet de Regions y no tiene un enlace que lo lleva a nuestra página oficial de Banca por Internet de Regions en [regions.com/espanol](https://www.regions.com/espanol), ignore el email y no divulgue ninguna información personal que le están pidiendo.
- Recuerde que nuestros emails siempre tendrán enlaces a páginas de Internet de Regions. Cuando nosotros hacemos un enlace a la Banca por Internet de Regions desde un email, la dirección en su navegador siempre aparecerá de esta manera:



- Cualquier email que usted reciba de Regions que tenga un enlace también incluirá los últimos cuatro dígitos de su número de cuenta para ayudarle a asegurar su autenticidad.
- Banca por Internet de Regions es una página de Internet segura, así que siempre habrá un candado cerrado en la parte inferior de su navegador. Por favor no divulgue ninguna información personal a una página de Internet que no muestre este candado: . Asegúrese de verificar las otras indicaciones que hemos listado aquí ya que este candado puede ser falsificado. Si tiene dudas, vaya directamente a [regions.com/espanol](https://www.regions.com/espanol) en una sesión separada.
- Regions no utiliza emails o ventanas tipo “popup” en la página de Banca por Internet de Regions para pedirle información.
- Cuando hacemos enlaces a programas desde nuestros emails, la información en la barra de dirección de página en su navegador siempre dirá “regions.com”.
- Los servidores de Regions están físicamente asegurados y monitoreados 24 horas al día. También están protegidos por firewalls de Internet.
- Es requerido ingresar a su cuenta antes de que tenga acceso a sus datos personales. Su PIN (Número de Identificación Personal) aparecerá como asteriscos cuando usted lo escriba.

- Para prevenir acceso no autorizado a sus cuentas cuando usted se levante y deje su computadora sola, su sesión de Banca por Internet de Regions termina automáticamente luego de 10 minutos. Es mejor que usted termine la sesión y cierre el navegador luego de completar su sesión bancaria.

## A Quien Puede Contactar si Usted es o Podría ser una Víctima de Robo de Identidad

Si usted comienza a recibir cuentas o llamadas sospechosas de acreedores con respecto a deudas que usted no conoce, usted podría ser la víctima de robo de identidad. Luego de verificar que el crédito sospechoso ha sido abierto usando su información personal, usted debe tomar los siguientes pasos:

1. Lo primero que debe hacer es llamar a la policía local y reportarlo. Asegúrese de recibir una copia del reporte de la policía. Le podrá hacer falta para convalidar sus reclamaciones.
2. Llame a todas las compañías de sus tarjetas de créditos e instituciones financieras para explicarles la situación. Cierre las cuentas problemáticas y abra cuentas nuevas. La información para contactar a Regions está en la próxima página.
3. Contacte al Departamento de Vehículos Motorizados local. A lo mejor querrá obtener una licencia de conducir nueva. Y debe verificar que no le hayan emitido a un impostor una copia de su licencia a su nombre.
4. Llame al Departamento de Seguro Social al 1-800-269-0271 si sospecha que usaron su número para obtener o abrir cuentas fraudulentas.
5. Pida que le pongan una alerta de fraude a sus reportes de crédito y revise cada reporte contactando a las 3 agencias de crédito:
  - Equifax: 1-800-525-6285
  - Experian: 1-888-EXPERIAN (397-3742)
  - TransUnion: 1-800-680-7289

6. Contacte a los Inspectores del Correo de EE.UU. o a su Correo local para reportar cualquier crimen relacionado con correspondencia robada o un crimen que ha usado correspondencia como parte de actividades fraudulentas.
7. Contacte a su compañía de seguro para notificarle del robo y para recibir una tarjeta de reemplazo. Los impostores pueden usar su tarjeta de seguro para obtener beneficios. Hasta su propia salud puede estar en riesgo si la información de salud de los impostores se añade a un perfil a su nombre si ellos reciben tratamiento.
8. Presente una queja con el FTC. Para presentar una queja o aprender más sobre las iniciativas de Robo de Identidad del FTC, visite [consumer.gov/idtheft](http://consumer.gov/idtheft). Si no tiene acceso al Internet, puede llamar al número de teléfono de Robo de Identidad del FTC (gratis): 1-877-IDTHEFT (438-4338); TDD (sordos): 866-653-4261; o mándeles una carta a:

Identity Theft Clearinghouse  
Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Washington, DC 20580

Use el **Registro de Acción Contra Robo de Identidad** que le proveemos en este paquete para documentar su proceso.

## Como Debería Manejar sus Cuentas de Regions

Primero debería revisar todas sus cuentas y buscar cualquier actividad o transacciones sospechosas en [regions.com/espanol](http://regions.com/espanol) o llamar al 1-800-REGIONS (734-4667).

Si usted ha determinado que sus cuentas de Regions no están seguras o sospecha que hay una cuenta de Regions que no abrió, por favor llame a un Representante de Regions al 1-888-987-6540. Si determina que no hay problemas con sus cuentas de Regions, le recomendamos que por favor:

- Le añade una contraseña de seguridad a todas las cuentas. Esto nos ayudará a nosotros a mantener su información protegida. Cada vez que nos llame por teléfono le pediremos su contraseña de seguridad.

- Revise la dirección, el número de teléfono y el email en sus cuentas para asegurar que tenemos la información correcta.
- Verifique que tiene en su posesión todos los cheques y las tarjetas emitidos bajo sus cuentas.

*Información adaptada de las agencias reguladoras del banco federal, cajas de ahorros y cooperativas de crédito.*

## Identity Theft Assistance Corporation (ITAC)

Regions es un Miembro que Fundó la Identity Theft Assistance Corporation (ITAC), la cual provee servicios gratis diseñados para disminuir el disgusto y los problemas que sufren las víctimas de robo de identidad. Si usted contacta a Regions para reportar un robo de identidad con respecto a una cuenta de Regions, ITAC le puede ayudar si está preocupado de que los pillos hayan abierto cuentas fraudulentas en otros bancos. ITAC también ha desarrollado un “Afidávit Estándar para Robo de Identidad”, el cual está incluido en este Paquete de Robo de Identidad. Al llenar el Afidávit Estándar para Robo de Identidad y el acuerdo de ITAC, usted recibirá ayuda de ITAC para resolver su reclamación de robo de identidad.

## Acuerdo y Descripción de Servicios de ITAC

El Centro de Ayuda de ITAC le puede ayudar a averiguar si ha ocurrido fraude en otras compañías financieras y lo pondrá en contacto con esas compañías.

Usted debe firmar y devolver esta página para poder usar los servicios de ITAC.

Al firmar más adelante, usted indica que leyó y entendió el Acuerdo y Descripción de Servicios de ITAC y que está de acuerdo con sus términos. Usted le da instrucciones y autoriza a ITAC y a cualquier compañía proveyendo servicios a nombre de ITAC a (1) obtener reporte(s) de crédito de agencias de reportes al consumidor, (2) presentar una alerta de fraude a su nombre con las agencias de crédito nacionales y (3) divulgar la información que ITAC reúne de usted y otras fuentes de otras compañías de servicios financieros, agencias del gobierno (como el FTC) y agencias de seguridad estatales y/o federales.

Firma \_\_\_\_\_

Fecha de Firma \_\_\_\_\_

Por favor llene y devuelva esta página con su firma y el Afidávit Estándar para Robo de Identidad por fax al (866) 209-5924 o enviándolo por correo a:

Regions Customer Protection Center  
ALBH70318A  
P.O. Box 413  
Birmingham, AL 35201

Si tiene cualquier pregunta, por favor llame al 1-888-987-6540.

# Afidávit Estándar para Robo de Identidad



## Información de la Víctima

1. Mi nombre completo legal es

\_\_\_\_\_  
(Nombre)      (Segundo Nombre)      (Apellido)      (Segundo Apellido\*)      (Jr., Sr., III\*)      \*Si aplica.

2. (Llene si aplica.) Cuando ocurrieron los eventos descritos en este afidávit, yo era conocido como

\_\_\_\_\_  
(Nombre)      (Segundo Nombre)      (Apellido)      (Segundo Apellido\*)      (Jr., Sr., III\*)      \*Si aplica.

3. Mi fecha de nacimiento es

4. Mi Número de Seguro Social es

\_\_\_\_\_  
Mes      Día      Año

5. Mi identificación emitida por el gobierno (pasaporte, licencia de conducir, identificación del estado, matrícula, visa, tarjeta de residencia permanente [“green card”]) es

Escoja una

Licencia de Conducir \_\_\_\_\_  
Estado      Número      Fecha de Emisión (mes/día/año)      Fecha de Expiración (mes/día/año)

Identificación del Estado

Pasaporte     Matrícula     Visa     Tarjeta de Residencia Permanente (“Green Card”)

\_\_\_\_\_  
Número      Fecha de Emisión (mes/día/año)      Fecha de Expiración (mes/día/año)

6. Mi dirección actual es

\_\_\_\_\_  
Número y Nombre de Calle      Afijo (Apartamento, Suite, etc.)

\_\_\_\_\_  
Ciudad      Estado      Código Postal

7. Mi dirección actual es \_\_\_\_\_  
Mes      Año

# Afidávit Estándar para Robo de Identidad



8. (Si es diferente a la anterior.) Cuando ocurrieron los eventos descritos en este afidávit, mi dirección era

Número y Nombre de Calle	Afijo (Apartamento, Suite, etc.)	
Ciudad	Estado	Código Postal

9. Yo viví en la dirección listada en el #8 desde \_\_\_\_\_ hasta \_\_\_\_\_  
Mes Año Mes Año

10. Mi número de teléfono durante el día es \_\_\_\_\_  
Mi número de teléfono durante la noche es \_\_\_\_\_  
Mi email es \_\_\_\_\_

## Como Ocurrió el Fraude

### Escoja todos los que apliquen para el #11 – #13

- 11.  Yo no autoricé a nadie que usara mi nombre o información personal para llevar a cabo transacciones financieras, cambiar cheques, hacer retiros u obtener dinero, artículos o servicios como están descritos en este reporte.
- 12.  Yo no recibí ningún beneficio, dinero, artículos o servicios como resultado de los eventos descritos en este reporte.
- 13.  Mis documentos de identificación (por ejemplo: tarjetas de crédito, certificado de nacimiento, licencia de conducir, tarjeta de Seguro Social, etc.):
  - todavía están en mi posesión     fueron robados en o alrededor del \_\_\_\_\_
  - se perdieron en o alrededor del \_\_\_\_\_  
Mes Día Año

# Afidávit Estándar para Robo de Identidad



Escoja el #14 ó #15 si aplica

14.  Según todo lo que yo sé y creo, la(s) siguiente(s) persona(s) usaron mi información (por ejemplo: mi nombre, dirección, fecha de nacimiento, números de cuenta existentes, Número de Seguro Social, apellido de soltera de madre, etc.) o documentos de identificación para llevar a cabo transacciones financieras, cambiar cheques, hacer retiros o para obtener dinero, artículos o servicios sin yo saber y sin mi autorización.

Name \_\_\_\_\_  
(Nombre) (Segundo Nombre) (Apellido) (Segundo Apellido\*) (Jr., Sr., III\*) \*Si aplica.

Dirección \_\_\_\_\_  
Número y Nombre de Calle Afijo (Apartamento, Suite, etc.)

Número(s) de Teléfono \_\_\_\_\_

Otra información \_\_\_\_\_

15.  Yo NO sé quien usó mi información o documentos de identificación para llevar a cabo transacciones financieras, cambiar cheques, hacer retiros o para obtener dinero, artículos, o servicios sin yo saber y sin mi autorización tal y como está descrito en este reporte.
16.  Comentarios adicionales (por ejemplo: descripción del fraude, documentos o información usados o cómo el pillo de robo de identidad llegó a tener acceso a su información).

## Opciones Legales de la Víctima

17. Escoja uno: YO  ESTOY  NO ESTOY dispuesto a asistir en iniciar una acción judicial contra de la(s) persona(s) que llevaron a cabo este fraude.
18. Escoja todos los que apliquen: YO  HE  NO HE reportado a la policía local los eventos descritos en este afidávit.  
Los policías  ESCRIBIERON  NO ESCRIBIERON un reporte. En el caso de que usted haya contactado a la policía u otra agencia de seguridad, por favor llene lo siguiente:

Departamento de Policía Número de Reporte, si aplica Fecha de Reporte (mes/día/año)

Número de Teléfono Email, si aplica

# Afidávit Estándar para Robo de Identidad



## Lista de Documentación

Por favor indique que tipo de documentación usted puede proveer para verificar su identidad. Adjunte copias (NO originales) al afidávit antes de mandarlo a su institución financiera.

- 19.  Una copia de una válida tarjeta de identificación con foto emitida por el gobierno (por ejemplo: su licencia de conducir, tarjeta de identificación emitida por el estado o su pasaporte).
- 20.  Prueba de residencia durante el tiempo que ocurrió la cuenta disputada, se hizo el préstamo u ocurrió el otro evento (por ejemplo: un acuerdo de renta/alquiler a su nombre, una copia de una cuenta de servicios o una copia de una cuenta de seguro).

## Firma

Yo certifico que, según todo lo que yo sé y creo, toda la información en y adjunta a este Afidávit es cierta, correcta y completa y hecha con intenciones honestas. Yo también entiendo que este Afidávit o la información que contiene estarán disponibles para agencias de seguridad federales, estatales y/o locales para tal acción legal dentro de su jurisdicción según ellos lo consideren apropiado. Yo entiendo que hacerle una declaración o representación falsa o fraudulenta al gobierno puede conllevar una violación del 18 U.S.C. § 1001 u otros estatutos criminales federales, estatales o locales y puede resultar en una multa, encarcelamiento o ambas.

Firma \_\_\_\_\_

Fecha \_\_\_\_\_

## Registro de Acción Contra Robo de Identidad de Regions

Este formulario sencillo le ayudará a mantenerse al tanto de su progreso mientras trabaja con los procesos diferentes. Asegúrese de ser detallado y preciso cuando esté listando la información y aún más importante, siempre dé seguimiento. Usted debe ser tan meticulouso como la gente que le robó su información.

### Contacto de Policía

Departamento de Policía	Número de Teléfono/ Dirección	Fecha(s) de Contacto	Nombre de Contacto	Notas

### Contactos de Cuenta Financiera

Banco/Tarjeta de Crédito/Inversión	Número de Teléfono/ Dirección	Fecha(s) de Contacto	Nombre de Contacto	Notas
Regions Bank	1-800-REGIONS (734-4667)			

### Departamento de Vehículos Motorizados

Departamento	Número de Teléfono/ Dirección	Fecha(s) de Contacto	Nombre de Contacto	Notas

## Departamento de Seguro Social

Departamento	Número de Teléfono	Fecha(s) de Contacto	Nombre de Contacto	Notas
Número de Emergencia del Depto. de Seguro Social	1-800-269-0271			

## Contactos de Agencias de Crédito

Agencia	Número de Teléfono	Fecha(s) de Contacto	Nombre de Contacto	Notas
Equifax	1-800-525-6285			
Experian	1-888-EXPERIAN (397-3742)			
TransUnion	1-800-680-7289			

## Federal Trade Commission

Departamento	Número de Teléfono	Fecha(s) de Contacto	Nombre de Contacto	Notas
Federal Trade Commission	1-877-IDTHEFT (438-4338) TDD (sordos): 866-653-4261			

## Contactos de Compañía de Seguro

Departamento	Número de Teléfono	Fecha(s) de Contacto	Nombre de Contacto	Notas
Federal Trade Commission	1-877-IDTHEFT (438-4338) TDD (sordos): 866-653-4261			

### Inspector del Correo de EE.UU.

Departamento	Número de Teléfono	Fecha(s) de Contacto	Nombre de Contacto	Notas

### Contactos de ITAC

Departamento	Número de Teléfono	Fecha(s) de Contacto	Nombre de Contacto	Notas



Cuenta con más.

1-800-REGIONS | [regions.com/espanol](http://regions.com/espanol)



© 2011 Regions Bank. Member FDIC.