



# ROBO DE IDENTIDAD

¿De qué  
se trata?

**Federal Trade Commission**

mayo 2003

Estimado Consumidor:

La Comisión Federal de Comercio (*Federal Trade Commission, FTC*) ha publicado el presente folleto para ayudarlo a tomar conciencia sobre el robo de identidad.

Si usted o alguien a quien conozca es víctima del robo de identidad, por favor visite [www.consumer.gov.idtheft](http://www.consumer.gov.idtheft). La información que usted ingrese, pasará a formar parte de una base de datos segura utilizada por funcionarios de todo el país a cargo del cumplimiento de la ley para colaborar en la tarea de detener las prácticas de los ladrones de identidad. El sitio Web de FTC también contiene vínculos con otras agencias federales y estatales y con organizaciones de consumidores.

También puede comunicarse con la Línea Directa de Asistencia de Robo de Identidad 1-877-ID THEFT, donde será atendido por consejeros que pueden ayudar a los consumidores que deseen o necesiten mayor información sobre cómo tratar las consecuencias del robo de identidad.

Lo alentamos a compartir este folleto con su familia, amigos, colegas y vecinos.

Atentamente,



J. Howard Beales, III  
Director  
Bureau of Consumer Protection  
Federal Trade Commission

# Contenido

---

Carta a los Consumidores

Introducción ..... 1

Cómo se Produce el Robo de  
Identidad ..... 2

¿Cómo Puedo Saber si Soy Víctima  
del Robo de Identidad? ..... 5

Cómo Manejar su Información  
Personal ..... 7

Comentario Especial sobre  
los Números de Seguro Social ..... 10

Si su Identidad Fue Robada ..... 14

Política de Privacidad de la FTC ..... 21



## Introducción

---

En la década del 90, apareció un nuevo tipo de estafador llamado ladrón de identidad. ¿Cuál es su mercadería de cambio? Las transacciones cotidianas de los consumidores que generalmente revelan algunos datos de su información personal: su número de cuenta bancaria y tarjeta de crédito, sus ingresos, su número de Seguro Social (SSN) o su nombre, domicilio y número de teléfono. Un ladrón de identidad obtiene algunos datos de su delicada información personal y, sin que usted lo sepa, se apropia de los mismos para cometer fraude o robo.

El robo de identidad es un delito serio. Las personas cuya identidad ha sido robada pueden perder meses o años — y también el dinero ganado con esfuerzo — reparando los perjuicios que los ladrones



han causado a sus registros de crédito y a su buen nombre. Algunas víctimas han perdido oportunidades de empleo, han sido rechazados para préstamos de estudios, vivienda o automóviles. Hasta en algunos casos, han sido arrestados por delitos que no cometieron.

¿Puede usted prevenir que se produzca el robo de identidad? Al igual que con otros delitos, usted no puede controlar completamente el hecho de convertirse en víctima del mismo. Pero, de acuerdo a la Comisión Federal de Comercio, usted puede minimizar su riesgo haciendo un manejo más cauto y de mayor sensibilidad de su información personal.

## **Cómo se Produce el Robo de Identidad**

Los “especialistas” en robo de identidad utilizan una variedad de métodos para acceder a sus datos. Por ejemplo:

- Obtienen información de negocios u otras instituciones:
  - robando registros de sus empleadores,
  - sobornando a un empleado para acceder a estos registros, o
  - “pirateando” — accediendo indebidamente — a las computadoras de las organizaciones.
- Revuelven y revisan la basura de su casa y de los negocios u obtienen información

a través de una práctica conocida como “búsqueda de basureros” (*dumpster diving*).

- Obtienen registros o informes de crédito ya sea aprovechándose del acceso autorizado por sus empleadores o haciéndose pasar por propietarios de vivienda, empleadores o alguna otra persona que pudiera tener un derecho legal a consultar la información.



- Roban números de tarjetas de crédito y débito cuando se procesa su tarjeta utilizando un dispositivo especial de almacenamiento de información a través de una práctica conocida como “*skimming*.”
- Roban bolsos y carteras conteniendo su identificación y sus tarjetas de crédito y bancarias.
- Roban correo, incluyendo resúmenes de cuenta bancarios y de tarjetas de crédito, ofrecimientos preaprobados de crédito, cheque nuevos o información de impuestos.
- Completan “formularios de cambio de domicilio” para derivar su correo hacia otra locación.

- Roban información personal de su casa.
- Le sacan engañosamente información fingiendo ser personas que operan legalmente un negocio o haciéndose pasar por funcionarios del gobierno.

Una vez que los ladrones de identidad tienen su información personal pueden:

- Salir de compras utilizando los números de su tarjeta de crédito y débito para comprar artículos de precios altos o “siderales,” tales como computadoras que pueden venderse fácilmente.
- Abrir una nueva cuenta de tarjeta de crédito utilizando su nombre, fecha de nacimiento y SSN. Al no pagar las facturas, la cuenta impaga vencida se reporta a su registro o informe de crédito.
- Cambiar el domicilio postal de su cuenta de tarjeta de crédito. Entonces, el impositor hace cargos sobre su cuenta. Debido a que las facturas son enviadas al nuevo domicilio, puede pasar un tiempo hasta que usted se dé cuenta de que existe un problema.
- Tomar préstamos a su nombre para comprar automóviles.
- Establecer servicios telefónicos convencionales o celulares a su nombre.

- Falsificar cheques o tarjetas de débito y vaciar su cuenta bancaria.
- Abrir una cuenta bancaria a su nombre y emitir cheques sin fondos sobre esa cuenta.
- Declararse en bancarrota o quiebra bajo su nombre para evitar pagar las deudas que contrajeron o para impedir un desalojo.
- Identificarse ante la policía con su nombre — el del consumidor — cuando son arrestados. En caso de que sean liberados de la custodia policial pero que no se presenten a la citación de la corte, se expide una orden de arresto nombre del consumidor defraudado.

## **¿Cómo Puedo Saber si Soy Víctima del Robo de Identidad?**

---

**A**lgunos indicadores del robo de Identidad pueden ser:

- no recibir facturas u otra correspondencia, lo que podría indicar que un ladrón de identidad hizo un cambio de domicilio;
- recibir tarjetas de crédito que usted no solicitó;
- denegación de crédito sin razón aparente; o

- recibir llamados de cobradores de deuda o compañías sobre mercaderías o servicios que usted no compró.

Solicite una copia de su informe de crédito a cada una de las principales agencias u oficinas de informes de crédito. Si el informe es correcto y contiene solamente aquellas actividades que usted autorizó, es probable que no sea una víctima del robo de identidad. La ley permite a las agencias cobrar hasta \$9 por una copia de su registro de crédito.

**Para ordenar sus informes de crédito:**

Equifax – [www.equifax.com](http://www.equifax.com)

1-800-685-1111

Experian – [www.experian.com](http://www.experian.com)

1-888-EXPERIAN (397-3742)

TransUnion – [www.transunion.com](http://www.transunion.com)

1-800-888-4213

# **Cómo Manejar su Información Personal**

---

• **¿**Cómo puede actuar un consumidor responsable para minimizar el riesgo y el daño potencial? Cuando se trate de su información personal, sea cauto y prudente.

## **HÁGALO YA**

Ponga contraseñas en sus tarjetas de crédito y bancarias y en sus cuentas telefónicas. Evite utilizar como contraseña información que sea de fácil disponibilidad como por ejemplo su apellido materno, su fecha de nacimiento, los últimos cuatro dígitos de su SSN, su número de teléfono o una serie de números consecutivos. Cuando al presentar una solicitud para una cuenta nueva le pidan su apellido materno, trate de reemplazarlo por una contraseña.

Resguarde su información personal dentro de su casa, especialmente si comparte la vivienda con otras personas o si recibe asistencia de empleados o servicios externos.

Consulte los procedimientos de seguridad implementados en su lugar de trabajo para resguardar la información personal. Averigüe quiénes tienen acceso a sus datos personales en su trabajo y verifique que los registros estén guardados en un lugar seguro. También pregunte cuáles son los procedimientos de eliminación de los



registros que contienen información personal.

#### DILIGENCIA COTIDIANA

No dé su información personal por teléfono, por correo o a través de Internet a no ser que sea usted quien haya iniciado el

contacto o sepa con quien está tratando. Con el objeto de hacerle revelar información de identificación, los ladrones de identidad pueden poner en práctica su talento para mentir y tal vez fingir ser empleados bancarios, Proveedores de Servicio de Internet (ISP) y hasta representantes de agencias gubernamentales. Confirme que está tratando con una organización legítima antes de compartir cualquier información personal. Verifíquelo llamando al servicio al cliente que se indica en su resumen de cuenta o en la guía telefónica.

Proteja su correo y su basura del robo. Deposite el correo que envía en buzones ubicados en oficinas postales o en la oficina postal local en vez de hacerlo en buzones no custodiados. Retire inmediatamente el correo de su buzón una vez que le haya sido entregado. Si tiene planes de

ausentarse de su casa por un tiempo y no pudiera recoger su correo, notifique al Servicio Postal de los Estados Unidos, 1-800-275-8777, y solicite el servicio de retención de correo. Para evitar que los ladrones puedan conseguir información a través de su basura o cestos de reciclaje, corte en pedazos sus recibos, copias de solicitudes u ofrecimientos de crédito, formularios de seguro, documentación médica, cheques y resúmenes bancarios y las tarjetas de crédito vencidas.

Antes de revelar cualquier información de identificación personal (por ejemplo, por medio de una solicitud), averigüe de qué manera será utilizada y protegida. También pregunte si la información brindada será compartida con terceros. Consulte si tiene opción sobre el uso que se le dará a su información: ¿Puede optar por mantener la información brindada como confidencial?

Conserve su tarjeta de Seguro Social en un lugar seguro y dé su SSN únicamente cuando sea absolutamente indispensable. Cuando sea posible, utilice otro tipo de identificación. Si en el Estado en el que reside se utiliza el mismo SSN para su licencia para conducir, solicite que lo sustituyan por otro.

Lleve consigo únicamente la información de identificación y la cantidad de tarjetas de crédito y débito que realmente necesita.

## **Comentario Especial sobre los Números de Seguro Social**

Su empleador e institución financiera muy probablemente necesitarán su número de Seguro Social (SSN) para fines de pagos de salarios y declaraciones de impuestos. Otros negocios privados pueden solicitarle su SSN para revisar su crédito, por ejemplo cuando solicita un préstamo para un automóvil. Sin embargo, algunas veces, solamente le solicitan ese número para sus registros. Si alguien le pide su SSN hágale las siguientes preguntas:

- ¿Porqué necesita mi SSN?
- ¿Cómo será utilizado mi SSN?
- ¿Cómo lo protegerá del robo?
- ¿Qué sucederá si no le doy mi SSN?

Algunos negocios pueden negarle la mercadería o servicio solicitado si usted no le informa su SSN. Obtener respuestas satisfactorias a estas preguntas lo ayudará a decidir si usted desea compartir su SSN con el negocio que se lo pida.

Esté atento a los períodos o ciclos de facturación. Si no recibe sus facturas en fecha, comuníquese con sus acreedores. Si su resumen de tarjeta de crédito no llega en la fecha habitual, esto podría indicar que un ladrón de identidad puede haberlo retenido y cambiado el domicilio de facturación para cubrirse al adueñarse de su cuenta.

Conserve su cartera o bolso en un lugar seguro en su trabajo.

#### PIENSE EN SU COMPUTADORA

Su computadora puede ser una mina de oro de información personal para un ladrón de identidad. Las siguientes recomendaciones pueden ayudarlo a mantener a resguardo su computadora y la información personal almacenada en la misma.

- Actualice su programa *software* antivirus regularmente. Los virus cibernéticos



pueden tener varios efectos perjudiciales, incluyendo la introducción en su computadora de un programa codificado que hace que la misma envíe archivos u otra información almacenada. Esté atento a las reparaciones de seguridad que puede descargar del sitio Web de su sistema operativo.

- No descargue archivos enviados por extraños y no pulse sobre hipervínculos desconocidos. Abrir un archivo podría exponer su sistema a un virus o programa de computación que puede ingresar a su módem sin su autorización.
- Use un programa *firewall*, especialmente si utiliza un acceso de “conexión permanente” a Internet. El programa *firewall* le permite impedir que los visitantes indeseados accedan a su computadora. Sin este programa, los *hackers* o piratas informáticos pueden acceder a su computadora y a su información personal almacenada en la misma.
- Utilice un navegador seguro — programa *software* que codifica o encripta la información que usted envía a través de Internet — para proteger la seguridad de sus transacciones en línea. Cuando someta información, busque el ícono del candado (*lock*) en la barra de estado el cual indica que su información se encuentra resguardada durante la transmisión.

- Trate de no almacenar información financiera en su computadora portátil a menos que sea absolutamente necesario. Si guarda este tipo de información, utilice una contraseña sólida — una combinación de letras (mayúsculas y minúsculas), números y símbolos.

Evite emplear la característica de conexión automática, la cual guarda su nombre de usuario y contraseña y no requiere que usted los ingrese cada vez que se conecta o que accede a un sitio en la red. Desconéctese siempre cuando termine. De esta manera, si le roban su computadora portátil será más difícil que el ladrón pueda acceder a su información personal.

- Antes de desechar una computadora, elimine toda la información personal almacenada. Utilice un programa de borrado o eliminación de archivos (*wipe*) para sobrescribir completamente el disco duro, de esta manera los archivos quedarán irrecuperables.
- Lea las políticas de privacidad de los sitios Web. Éstas deberían dar respuesta a sus inquietudes sobre la manera en que mantienen la precisión, acceso, seguridad y control de la información personal recogida por el sitio y también cómo será utilizada y si será provista a terceros.

## **Si su Identidad Fue Robada**

---

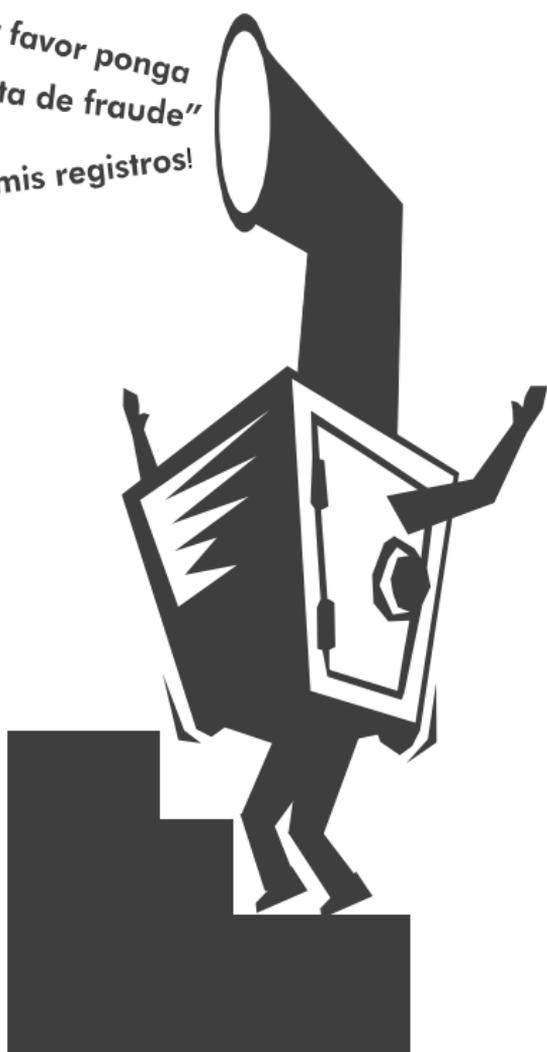
**A**unque usted haya sido muy cuidadoso manteniendo su información personal de forma confidencial, un ladrón de identidad puede aún atacar. Si usted sospecha que su información personal ha sido utilizada para cometer fraude o robo, **tome inmediatamente las cuatro medidas que se detallan a continuación.** Recuerde hacer un seguimiento por escrito de todos los llamados telefónicos; envíe su correspondencia por correo certificado con acuse de recibo (*return receipt*), de manera de poder documentar la fecha de recepción de su carta y conserve copias para sus registros.

### **1. Tome contacto con los departamentos de fraude de las tres compañías principales de informes de crédito.**

- **Equifax** — Para reportar un fraude llame a: 1-800-525-6285 y escriba a: P.O. Box 740241, Atlanta, GA 30374-0241
- **Experian** — Para reportar un fraude llame a: 1-888-EXPERIAN (397-3742) y escriba a: P.O. Box 9532, Allen TX 75013
- **TransUnion** — Para reportar un fraude, llame a: 1-800-680-7289 y escriba a: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Dígales que usted ha sido víctima de un robo de identidad y solicíteles que incluyan una “alerta de fraude” en su registro y también una “declaración de la víctima.” Esto indica a los acreedores y otorgantes de crédito que se comuniquen con usted antes de abrir cualquier cuenta nueva o antes de efectuar cambios sobre las cuentas existentes y también ayuda a evitar que un ladrón de identidad continúe abriendo cuentas adicionales a su nombre. Al mismo tiempo, solicite copias de sus informes crediticios. Las agencias de informes de crédito deberán proporcionarle estas copias sin cargo

*¡Sí, por favor ponga  
una “alerta de fraude”  
en mis registros!*



alguno en caso de que su informe sea inexacto o que usted haya sufrido fraude y en tanto usted haga la solicitud por escrito.

Revise sus informes de crédito cuidadosamente para asegurarse que la información que contienen es correcta. Busque investigaciones o averiguaciones que usted no inició, cuentas que no abrió y deudas inexplicables sobre sus cuentas reales. También debería revisar que datos tales como su SSN, domicilio(s), nombre o inicial y empleadores estén listados correctamente. Las inexactitudes también pueden deberse a errores tipográficos. No obstante, ya sea que se trate de inexactitudes por fraude o por error, notifique a las agencias de informes crediticios por teléfono y por escrito lo antes posible. Deje pasar unos pocos meses y ordene nuevas copias de sus registros — tanto para verificar las correcciones y cambios que usted hizo como también para asegurarse de que no se desarrolló nuevamente actividad fraudulenta.

Las “alertas de fraude” y “declaraciones de las víctimas” son servicios voluntarios provistos por las agencias de crédito. Los acreedores no tienen que considerarlos al momento de otorgar un crédito. Por esta razón, es de vital importancia continuar revisando sus informes periódicamente. Además, las alertas de fraude y declaraciones de las

víctimas expiran y es necesario que las renueve periódicamente. Consulte las políticas sobre este tema con cada agencia.

## **2. Cierre aquellas cuentas que usted sepa o crea que han sido falsificadas o abiertas fraudulentamente.**

### **Cuentas de Crédito**

Las cuentas de crédito comprenden todas las cuentas bancarias, de compañías de tarjetas de crédito y otras entidades de préstamos y compañías de teléfono, servicios públicos, Proveedores de Servicio de Internet (ISP) y otros proveedores de servicios.

Si usted cierra sus cuentas existentes, utilice nuevos números de identificación personal (PIN) y contraseñas al abrir nuevas cuentas.

Si se presentan cargos o débitos indebidos o fraudulentos, consulte a la compañía sobre los siguientes formularios para disputar dichas transacciones:

Para cuentas nuevas no autorizadas pregunte si la compañía acepta la Declaración Jurada de Robo de Identidad (*ID Theft Affidavit*), (disponible en Internet visitando: [www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf](http://www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf)). Si no la acepta, solicite al representante que le envíe los formularios de disputa de fraude de la compañía.

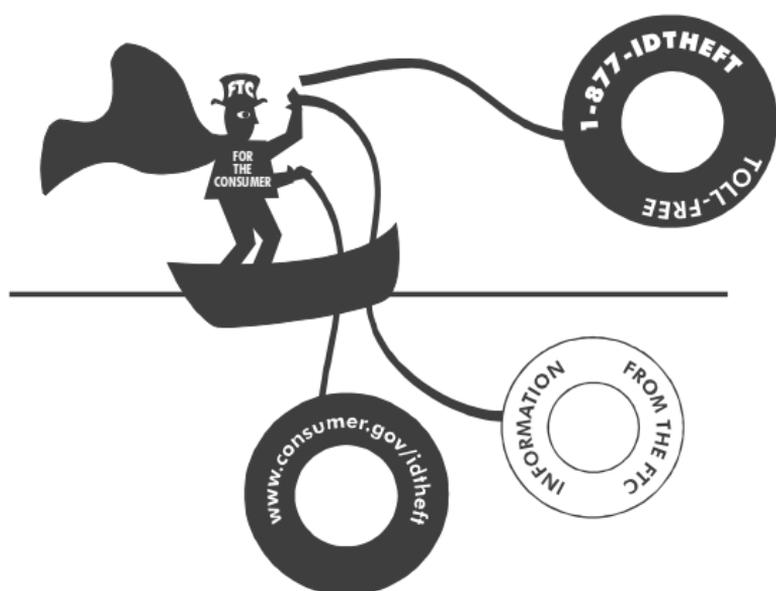
Para cuentas existentes, pida a un representante que le envíe los formularios de disputa de fraude de la compañía.

Si su tarjeta de cajero automático (ATM) se perdió, fue robada o comprometida de alguna otra manera, cancele la tarjeta tan pronto como le sea posible. Obtenga una nueva tarjeta con un nuevo número de identificación personal (PIN).

### *Cheques*

Si sus cheques fueron robados o malversados, suspenda los pagos y solicite a su banco que notifique al servicio de verificación de cheques correspondiente. Aunque ninguna ley federal limita sus pérdidas si alguien roba sus cheques y falsifica su firma, las leyes estatales pueden protegerlo. La mayoría de las leyes estatales hacen responsable al banco por las pérdidas producidas por un cheque falsificado, pero también requieren que usted haga un uso cuidadoso de su cuenta bancaria. Por ejemplo, usted puede ser considerado responsable por la falsificación si no notifica con tiempo al banco cuando un cheque fue robado o perdido. Contacte la agencia estatal bancaria o de protección del consumidor para obtener más información.

Usted puede contactar a las principales compañías de verificación de cheques. Solicíteles que informen a los



comerciantes que utilizan la base de datos de la compañía que no acepten sus cheques.

**TeleCheck** —

1-800-710-9898 ó 927-0188

**Certegy, Inc.** —

1-800-437-5120

**International Check Services** —

1-800-366-5010

Llame a SCAN (1-800-262-7771) para averiguar si un ladrón de identidad ha pasado cheques suyos sin fondos o falsificados.

- 3. Presente una denuncia o informe en la dependencia policial local o en la de la comunidad donde haya ocurrido el robo de identidad.**

Conserve una copia de la denuncia policial ya que puede necesitarla para autenticar sus quejas ante los acreedores. Si no puede obtener una copia de la denuncia, al menos consiga el número de la misma.

#### **4. Presente una queja ante la FTC.**

Visite [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft) para presentar una queja instantáneamente, obtener una copia de la Declaración Jurada de Robo de Identidad y obtener respuestas a las preguntas más frecuentes sobre este tema. Si no tiene acceso a Internet llame a la Línea Directa de Robo de Identidad: 1-877-IDTHEFT (438-4338). Su queja será ingresada a una segura base de datos de fraude a los consumidores a la cual pueden acceder únicamente las agencias a cargo del cumplimiento de la ley con propósitos de realizar investigaciones penales.

## **POLÍTICA DE PRIVACIDAD DE LA FTC**

La FTC ingresa la información que usted envía a su base de datos segura — Cámara Compensadora de Datos de Robo de Identidad (*Identity Theft Clearing House*) — y la comparte con sus abogados e investigadores. La información también puede ser compartida con empleados de varias otras autoridades federales, estatales o locales de seguridad o regulación. También podemos compartir parte de la información con ciertas entidades privadas, como agencias de informes de crédito y aquellas compañías sobre las cuales usted pudo haber presentado una queja, en caso de que creamos que al hacerlo estamos colaborando en la resolución de problemas relacionados con el robo de identidad. Usted puede ser contactado por la FTC o por cualquiera de las agencias o entidades privadas a las cuales se haya derivado su queja. En otras limitadas circunstancias, incluyendo solicitudes del Congreso, se nos puede requerir por ley que revelemos la información que usted nos someta.

Usted tiene la opción de enviar su información anónimamente. Sin embargo, si usted no provee su nombre e información de contacto, las agencias a cargo del cumplimiento de la ley y otras entidades no podrán contactarlo para obtener información adicional que podría ser de ayuda para las investigaciones y procesamientos de robo de identidad.

LUISA ADRIANA LAURA PATRICIA

SMAEL YARA GENARO LOUISA

JUAN DANIEL ANNA NOE MARCELA

PILAR CRISTINA HUMBERTO EMILIA

JORGE DAVID RAFAEL CHUY JUAN

CAROLINA ESPERANZA LUZ ELIZABETH

AMANDA NOELIA ABEL LEONARDO

ROBERTO MARTA MARIA JOSE

ANDREA SANDRA ALICIA GABRIELA

CARLO FERNANDO YARA CAROLINA

1-877-ID-THEFT (1-877-438-4338)

ROSALBA SUSANA SARA JULIAN

[www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)

FLAVIA CESAR ROBERTO DAMIAN