

Servicios Legales de Puerto Rico, Inc.  
Proyecto Justicia para el Consumidor

**ROBO DE IDENTIDAD**

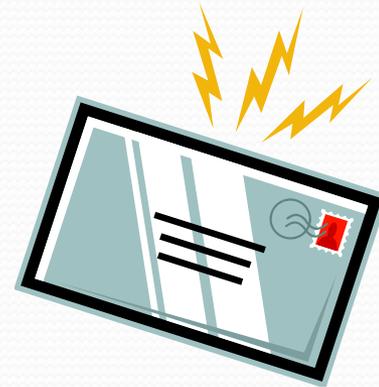
# DEFINICIÓN

- Robo de identidad es cuando alguien usa información personal de otra persona para hacerse pasar por ese consumidor con el fin de:
  - **Obtener bienes y servicios a nombre de la víctima de manera fraudulenta. (Tanto de instituciones públicas como privadas.)**
  - **Ocultar su verdadera identidad de las autoridades y de otras instituciones que realizan “background checks”.**



## Robo de Identidad (*métodos antiguos*)

- Carteras perdidas o robadas.
- Robo perpetrado por familia o amigos.
- Obteniendo información personal en la basura.
- Robo de correspondencia.
- A través de algún empleado de un banco, de un hotel o de cualquier otro negocio.



## ...utilizando alta tecnología



- “*skimming*”- cuando se copia la data que se transmite electrónicamente en la cinta magnética de una tarjeta de crédito.
- “*data breaches*”- irrumpir en sistemas de computadora.
- “*phishing*”- es el envío de un correo electrónico con apariencia de ser auténtico diseñado para engañar al que lo recibe con el fin de que ofrezca información personal.

# ALGUNAS MODALIDADES

- Financiera
- Niños
- Teléfonos inteligentes
- Empleo
- Médica



# FINANCIERA

- Presentar querrela a la policía y pedir copia de la misma. Una vez tenga esta querrela, la víctima tiene derecho a:
  - ✓ Alerta de fraude por 7 años.
  - ✓ “Credit freeze” (donde aplique)
  - ✓ Bloquear información fraudulenta del informe de crédito.

# Continuación... Financiera

- ✓ Recibir copia de todos los récords de solicitudes y transacciones de la cuentas abiertas fraudulentamente a nombre de la víctima.
- ✓ Que la cuenta se remueva del informe de crédito una vez la víctima haya suministrado evidencia de que la misma es fraudulenta. Esto incluye paralizar cualquier acción de cobro.

# ORGANIZACIÓN DEL CASO

- Mantener récord de llamadas hechas y recibidas.
- Toda la correspondencia cursada debe ser enviada por correo certificado.
- Todos los acuerdos deben hacerse por escrito.
- Guardar todos los recibos de gastos y copia de toda la correspondencia enviada y recibida.



# TRABAJAR CON LA PERSONA CORRECTA

- Hablar con funcionarios del área de investigación y fraude de la compañía.
- La Administración del Seguro Social se involucra a través de su oficina del Inspector General, solamente si hay fraude en los beneficios o robo de cheques.
- Querrela en la policía.

## Continuación... Trabajar con la persona correcta

- El Servicio Secreto y el FBI intervienen únicamente a petición de la policía de la oficina o del U.S. Attorney General.
- Cuando se trate de robo de correspondencia o fraude postal debe hablar con el “Postal Inspector Office”, no con el gerente del correo local.
- En el Departamento de Vehículos de Motor debe contactar al investigador de fraude.

# EVALUAR EL DAÑO / PRIMEROS PASOS

- Tarjetas de crédito, cheques y tarjetas atm robadas
  - ✓ Contactar institución financiera, cerrar cuentas y poner contraseñas.
- “Account takeover”
  - ✓ Cerrar cuenta y abrir otra. Actuar rápido y revisar estados de cuenta, poner contraseñas.
- Número de Seguro Social
  - ✓ Pedir informes de crédito y alertar sobre el fraude en la misma solicitud.

# RECUPERACIÓN

- Contactar policía y hacer querrela.
- Contactar a todos los acreedores, compañías y agencias de cobro que abrieron cuentas fraudulentas.
- Obtener récord de las transacciones.
- Contactar agentes investigativos y proveerles toda la información obtenida.

# Continuación ... Recuperación

- Contactar agencias de información de crédito para completar documentación necesaria para la corrección de errores.
- Obtener “clearance letters” de los acreedores.
- Verificar que se hayan hecho las correcciones en los informes de crédito.
- “Credit freeze” (si está disponible)

# NIÑOS

- Ocurre cuando la identidad de un niño es usada por otra persona para su propio beneficio.
- El impostor puede ser un miembro de la familia, algún conocido o un extraño.
- Las víctimas de este crimen son:
  - ✓ Adultos/niños- adultos que se enteran de que su identidad fue robada cuando eran niños.
  - ✓ Niños- niños que tienen un familiar adulto que se percata del crimen.



# DESCUBRIMIENTO

- **Niños**- padres descubren que hay cuentas de banco abiertas con el número de seguro social del menor.
- Reciben tarjetas de crédito pre aprobadas, cheques y estados de cuenta a nombre del menor.
- Llamadas de agencias de cobro.
- Cuando a un adolescente le deniegan la solicitud de la licencia de conducir.
- Órdenes de arresto a nombre del niño.

# Continuación...

- **Adulto/Niño**- se entera cuando le deniegan préstamos, hipotecas o tarjetas de crédito.
- No pueden abrir cuentas.
- Reciben cartas o llamadas de cobro.
- Se le deniegan servicios (utilidades), renovación de la licencia de conducir.
- Despedidos del empleo sin razón aparente.
- Reciben cuentas o tarjetas de crédito que nunca solicitaron.
- Arrestos.
- Se le deniegan beneficios de Seguro Social o de bienestar social.

# CURSO DE ACCIÓN

- Cuando se trata de *niños*, los padres tienen que actuar a su favor.
- Solicitar informe de crédito
- Reportar el crimen a la policía.
- Contactar a los acreedores para eliminar los récords del menor.

Continuación...

## CURSO DE ACCIÓN

- Certificado de nacimiento.
- Hablar solamente con investigadores de fraude.
- Organizar documentación.
- Comunicarse con agencias de cobro.

# Continuación...

## CURSO DE ACCIÓN

- Enfatizar que la víctima es menor de edad y que no lo pueden contactar.
- Solicitar que todas las cuentas solicitudes y gestiones de cobro sean removidas del informe de crédito del menor.
- Solicitar copia de todas las transacciones y entregarlas a la policía.
- Cuando se trata de adultos a los que se les robó la identidad cuando eran menores, se siguen los mismos pasos que seguirían con cualquier otro adulto.

# ¿Puede cambiarse el número del Seguro Social?

- La Administración del Seguro Social tiene criterios muy estrictos para otorgar un número nuevo. No obstante, un joven adulto podría beneficiarse del cambio.

# TELÉFONOS INTELIGENTES

- Un teléfono inteligente es aquel con capacidad ampliada.
- Con el incremento en la capacidad de los teléfonos, también aumenta el riesgo de exponer información personal.



# RIESGOS

- Se pierden o se los roban.
- Están asociados al usuario para propósitos de facturación, entre otros.
- Mayor exposición. (wi-fi)
- Algunas aplicaciones no son seguras. (“phishing”)

# PREVENCIÓN

- Contraseñas.
- Instalar programas de seguridad.
- Estar pendiente de lo que hace en el teléfono. (no abrir enlaces sospechosos, asegurarse de que los sitios son seguros antes de dar información personal)
- Ser cuidadoso con las aplicaciones que instala.
- Instalar una aplicación para encontrar el telefono si se pierde o lo roban.
- Limitar el uso de Wi-fi público.
- Verificar URLs antes de hacer compras usando su teléfono.

# Si pierde el teléfono...

- Llamar de inmediato al proveedor de su servicio de teléfono móvil, cancelar el servicio y reportar la pérdida.
- Comunicarse con el administrador de su programa y borrar el teléfono.

# Robo de Identidad...EMPLEO

- Uso de la información de identificación personal de la víctima para obtener y retener un empleo.
- Usualmente se descubre a través de una notificación del IRS o cuando se le deniega algún beneficio público.

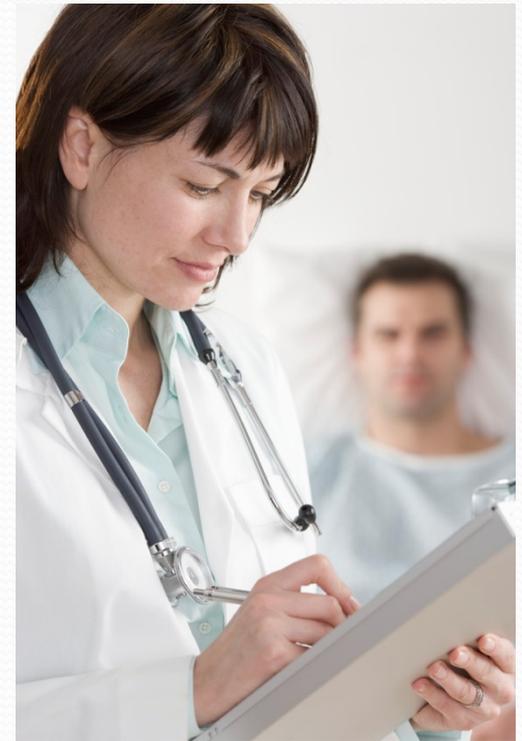


# Cómo ayudar a la víctima...

- Obtener copia en el Seguro Social de los registros de ingreso de la víctima.
- Identificar la actividad del impostor y solicitar que los registros sean corregidos.
- Entregar el registro de ingresos corregido junto a cualquier otro documento al IRS.
- Solicitar que el número de Seguro Social de la víctima sea señalado (“flagged”).

# Robo de Identidad Médica

- Ocurre cuando un impostor utiliza la identidad de otra persona, o su plan médico para recibir cuidado médico.
- Muy peligroso porque los expedientes médicos del impostor se unen con los de la víctima.
- Difícil de remediar debido a la Ley HIPAA.



# Como ayudar a la víctima...

- Reportarlo a las autoridades y obtener copia de la querrela.
- Solicitar al médico primario los récords médicos de la víctima con el fin de usarlos como punto de referencia para comparar.
- Solicitar los récords médicos de la víctima y las políticas de privacidad a cada proveedor que atendió al impostor.  
(importante: en este punto no se debe mencionar el robo de identidad)
- Revisar los récords y escribirle a los proveedores para que corrijan y establezcan alertas.
- Confirmar que los récords en efecto, fueron corregidos.

## La víctima va a necesitar abogado cuando....

- Su edad, salud, manejo del lenguaje y su situación económica afecte su representación por derecho propio.
- Han sido demandados u hostigados por acreedores tratando de cobrar las deudas en las que incurrió el impostor.
- Los acreedores y las agencias de reportes de crédito no cooperan.
- Para garantizarle los derechos cuando la persona que les robó la identidad sea arrestada.
- Su caso es complejo.



Las víctimas necesitan un abogado para vindicar sus derechos al amparo de las siguientes leyes...

- Fair Credit Reporting Act (FCRA)
- Fair Credit Billing Act (FCBA)
- Electronic Fund Transfer Act (EFTA)
- Fair Debt Collection Practices Act (FDCPA)
- Child and Family Services Improvement and Innovation Act of 2011.

# Otros Recursos

- Internal Revenue Services- Identity Protection Specialized Unit (1-800-908-4490)
- Social Security Administration- 1-800-772-1213  
[www.ssa.gov/pubs/10064.html](http://www.ssa.gov/pubs/10064.html)
- Federal Trade Commission- [www.ftc.gov/bulkorder](http://www.ftc.gov/bulkorder)  
<http://www.idtheft.gov>

# REFERENCIAS

- <http://www.idtheftcenter.org>
- FTC Webinar on ID Theft, June 2013.



Financiado por la  
Legal Services Corporation

# Servicios Legales de Puerto Rico, Inc. Proyecto Justicia para el Consumidor



“ Este programa recibió fondos especiales del Departamento de Justicia. Los puntos de vista u opiniones vertidas en estos documentos son del autor y no necesariamente representan la posición oficial y la política del Departamento de Justicia”

