Protéjase contra el robo de identidad

El robo de identidad ocurre cuando alguien obtiene y utiliza fraudulentamente la información personal de otra persona (nombre, fecha de nacimiento, número de seguro social, etc.) para asumir la identidad de esa persona. Esto incluye robo de dinero u obtener artículos u otros beneficios pretendiendo ser otra persona. Es un crimen utilizar la identidad de otra persona.

¿Cómo puede proteger su información personal?

Existen varias medidas básicas que puede tomar para disminuir o minimizar el riesgo de llegar a ser víctima de robo o fraude de identidad:

- Proteja su número de Seguro Social *(SSN, Social Security Number)*, números de tarjetas de débito y tarjetas de crédito, números de identificación personal *(PINs, personal identification numbers)*, contraseñas y demás información personal.
- Dé su número de seguro social únicamente cuando sea absolutamente necesario y pregunte si puede usar otras clases de documentos de identidad.
- Cree un identificador de cliente *(Customer ID)* único (en vez de su SSN) al acceder la información de su cuenta siempre que sea posible, incluso en el sitio Web de Diversified.
- Proteja el correo que recibe y que envía. No deje el correo en su buzón de correo sin llave por un largo período de tiempo.
- No dé su información personal por teléfono, por correo o en Internet a menos que sea usted quien haya iniciado la llamada o esté seguro de que sabe con quién está tratando.
- Destruya cualquier documento que contenga su información financiera antes de botarlo a la basura. Rompa o corte recibos, copias de solicitudes de crédito, formularios de seguros, cheques y estados de cuenta bancarios, tarjetas de crédito vencidas y ofrecimientos de crédito.
- Mantenga estrecha vigilancia sobre sus estados de cuenta bancarios y las cuentas de las tarjetas de crédito en busca de irregularidades.
- Actualice su software de protección antivirus con regularidad e instale las correcciones de seguridad necesarias.
- No abra archivos que le envíen personas extrañas ni haga clic en los hiperenlaces *(hyperlinks)* en los mensajes de correo electrónico (siempre digite usted mismo la dirección electrónica).
- Utilice un programa cortafuegos *(firewall)*, especialmente cuando use una conexión de Internet de alta velocidad.
- No utilice una opción de ingreso *(sign-in)* automática que almacena su nombre y contraseña, y siempre cierre su conexión cuando termine.
- Busque la política de privacidad de la página web y léala, tal como la política de privacidad del sitio web de Diversified. La política de una compañía debería contestar preguntas sobre el mantenimiento de la exactitud, acceso, seguridad y control de la información personal que se obtiene a través del sitio. Además debería contestar cómo se usará la información y si ella se suministrará a terceros. Si no ve una política de privacidad o si no la entiende, considere no hacer negocios con esa compañía.
- Si necesita suministrar su información personal o financiera a través del sitio web de una organización, busque un indicador de que el sitio es seguro. Por ejemplo, un ícono de candado en la barra de estatus del buscador o una dirección electrónica de un sitio web que empieza con “https:”, en donde la “s” significa “seguro”.

DIVERSIFIED
Partners in Retirement Solutions

Protéjase contra el robo de identidad

¿Cuáles son las señales de alerta del robo de identidad?

Las señales pueden incluir:

- De repente dejan de llegar sus estados de cuenta bancarios y de tarjetas de crédito.
- Aparecen en sus estados de cuenta cargos o retiros no autorizados.
- Le niegan una solicitud de crédito, sin razón aparente.
- Empieza a recibir cuentas de compañías que usted no reconoce.
- Las agencias de cobros tratan de cobrarle deudas que no son suyas.
- Recibe tarjetas de crédito que no ha solicitado.
- Es incorrecta la última fecha de ingreso *(last sign-in date)* que muestra un sitio Web que tiene su información personal.

¿Qué puede hacer si sospecha un robo de identidad?

Si sospecha que su información personal se ha utilizado fraudulentamente, de inmediato:

- Ponga una alerta de fraude a sus reportes de crédito, llamando a una de las tres agencias de crédito: Equifax (1-888-766-0008), Experian (1-888-397-3742) y TransUnion (1-800-680-7289). Una alerta de fraude inicial permanece en su reporte de crédito por al menos 90 días.
- Solicite un informe de crédito actualizado en **annualcreditreport.com** y busque algún préstamo nuevo (ejemplo; para casa, automóvil, escuela, etc.) tomado a su nombre, o cuentas de tarjeta de crédito nuevas que usted no abrió. Cierre dichas cuentas inmediatamente.
- Coloque una congelación de crédito en su archivo de crédito llamando a las tres agencias de crédito. La congelación evita que los prestamistas vean su reporte a menos que usted autorice el acceso y puede prevenir que otros tomen créditos nuevos a su nombre, aún si poseen su número de seguro social (SSN) y demás información personal.
- Realice un reporte de fraude en su departamento de policía local.
- Llene en Internet (en español) una queja con la Federal Trade Commission en **http://www.ftc.gov/bcp/edu/microsites/idtheft/en-espanol/index.html** y seleccione “Presente una queja”.
- Llame a Diversified y a cualquier otra institución para iniciar el proceso de asegurar sus cuentas.

Para obtener más información sobre cómo protegerse contra el robo de identidad, visite el sitio web de la Federal Trade Commission en **http://www.ftc.gov/bcp/edu/microsites/idtheft/en-espanol/index.html**.

Para obtener información adicional sobre su cuenta de jubilación en Diversified, visite **divinvest.com** (transacciones en inglés) o llame en español al **1-800-755-5801**.

PT-5696-S (02/12) © 2012 Diversified Retirement Corporation