OREGON
Identity Theft Protection Act

Protección de información personal

Guía para negocios

DEPARTMENT OF CONSUMER & BUSINESS SERVICES

Division of Finance and Corporate Securities

Ley de Oregon de Protección contra el robo de la identidad

Recopilar y obtener datos de información personal es fundamental para todos los tipos de empresas, organizaciones y entidades gubernamentales, grandes y pequeñas. La mayoría de las organizaciones, tanto públicas como privadas, obtienen información personal, como nombres, direcciones, números de tarjetas de crédito y del Seguro Social manual o electrónicamente (o ambos) para realizar transacciones y dirigir mejor sus productos y servicios a posibles clientes.

Sin embargo, si esa información cae en manos de personas deshonestas, puede ser explotada por los que cometen robo de identidad. El robo de identidad puede crear una gran confusión económica tanto para las empresas como para el público. De acuerdo a la Comisión Federal de Comercio, este delito cuesta cerca de 48 mil millones de dólares a las empresas cada año. Oregon está clasificado como el 13° peor del país en robo de identidad, lo cual puede ser especialmente perjudicial para las empresas pequeñas con recursos limitados.

Oregon tiene una nueva ley — la Ley de Oregon de Protección Contra el Robo de Identidad — que le dará orientación y expectativas claras para garantizar la seguridad de datos delicados. Los consumidores de Oregon tendrán más herramientas para protegerse contra el robo de identidad al tener la opción de poner un congelamiento de seguridad en sus archivos de crédito.

⚠ *Su responsabilidad...*

Usted puede evaluar y minimizar los riegos para su empresa y para los consumidores siguiendo los requerimientos contenidos en la Ley de Oregon de Protección Contra el Robo de Identidad, promulgada en el 2007. La ley contiene normas para proteger el número del Seguro Social, notificar a los consumidores en casos de violaciones de seguridad y salvaguardar la información personal de identidad.

En reconocimiento de que Oregon tiene un alto porcentaje de pequeñas empresas, los componentes de la ley se pueden adaptar y aplicar independientemente ya sea que tenga 5 o 500 empleados.

El Departamento de Servicios para Consumidores y Negocios está a cargo de hacer cumplir estas nuevas leyes y de proporcionar materiales educativos.

La protección de los números del Seguro Social

El número del Seguro Social (SSN) es el medio más específico de identificación de una persona porque nunca cambia. A diferencia de otra información de identificación, el SSN desempeña un papel significativo en vincular datos que contienen información delicada. Este factor exclusivo es lo que hace que un SSN sea tan valioso para los que cometen robo de identidad. Tanto el uso generalizado de este número de identificación como su valor han contribuido al incremento del robo de identidad y al fraude de crédito.

⚠ *Su responsabilidad...*

La Ley de Oregon de Protección Contra el Robo de Identidad prohíbe que cualquier persona, agencia del gobierno, organización o empresa imprima números de Seguro Social en cualquier material que es enviado por correo sin que el propietario de éste lo haya pedido. Esto no es aplicable a archivos o documentos requeridos bajo la ley estatal o federal tales como W2s, 1099s o documentos similares. La ley también prohíbe la impresión de los números de Seguro Social en tarjetas que el consumidor utiliza para obtener productos o servicios, también prohíbe que dichos números sean publicados o mostrados públicamente, por ejemplo en un sitio Web. Esto no es aplicable a récords que son requeriedos bajo la ley estatal o federal para propósitos internos de verificación o procesos administarativos, o que son usados para hacer cumplir ordenes de los juzgados o de las cortes.

Otras excepciones son:

- Reglas adoptadas por las cortes
- Copias de datos poseídos por una corte, el administrador de la Corte del Estado o el Secretario de Estado

Las empresas u organizaciones que empleen el SSN como un identificador de una cuenta, deben emplear otros medios para identificar la cuenta del consumidor.

Notificación a los consumidores

Cuanto antes sepa un consumidor que su identificación ha sido expuesta mayores son sus oportunidades de asegurar que esa información no se use de manera fraudulenta.

La información personal incluye el nombre de un consumidor junto con un número del Seguro Social, el número de la licencia de conducir de Oregon o de la tarjeta de identificación de Oregon, el número de una tarjeta financiera, de crédito o de débito junto con un código o contraseña de seguridad o número de identificación personal (PIN) que puedan permitir que alguien tenga acceso a una cuenta financiera de un consumidor.

⚠ *Su responsabilidad...*

Los que mantienen información personal tienen que notificar a los consumidores lo antes posible de una de las siguientes maneras si es que archivos computarizados que contienen información personal han sido objeto de una falla de seguridad:

- Notificación por escrito
- Notificación electrónica si ésta es la manera de comunicación habitual entre usted y sus clientes
- Notificación por teléfono, si usted hace contacto directo con el consumidor afectado

Una persona o empresa que mantenga o posea información personal en nombre de otra persona o empresa debe notificar inmediatamente al propietario o titular de una licencia que hubo una falla de seguridad.

La notificación a los consumidores se puede aplazar o prorrogar si una entidad de cumplimiento de la ley determina que la notificación dificultará una investigación criminal.

Si una investigación de la violación o la consulta con una entidad federal, estatal o local de cumplimiento de la ley determina que no hay probabilidad razonable de que la falla de seguridad haga daño a los consumidores, o si la información personal fue codificada o hecha ilegible, no se requiere notificación.

Toda persona, empresa, agencia del gobierno u organización sujeta a, y que cumpla con las regulaciones de notificación u orientación adoptadas por la Ley Gramm-Leach-Bliley, HIPPA, cumple con los requerimientos de notificación de Oregon. No obstante, si la falla tiene que ver con los empleados de la empresa, esta deberá cumplir con los requerimientos de notificación de Oregon.

Notificación alternativa

Si usted demuestra que el costo de notificar a los consumidores excedería $250,000, que el número de consumidores que deben ser contactados supera los 350,000 o si no tiene los medios económicos suficientes para ponerse en contacto con los consumidores, se permite dar notificación alternativa, tal como:

- La exhibición conspicua de la notificación o de un enlace de la notificación en su sitio Web, si mantiene uno, y
- La notificación por medio de los principales canales de televisión y diarios de Oregon que estén disponibles en todo el estado.

Notificación a las entidades de reportes de crédito

En el caso de que la falla de seguridad afecte a más de 1,000 consumidores, la persona u organización responsable por la falla debe informar a las tres agencias de reporte crediticio (TransUnion, Equifax, Experian) sin demora, la fecha, la distribución y el contenido de la notificación provista a los consumidores afectados.

Protección de datos

Los consumidores aprecian los productos y servicios que usted les proporciona; también apreciarán las medidas que usted tome para proteger con efectividad la información personal que los identifique.

> ⚠ ***Su responsabilidad...***
>
> La Ley de Oregon de Protección Contra el Robo de Identidad requiere que usted establezca, implemente y mantenga salvaguardas razonables para garantizar la seguridad, confidencialidad e integridad de la información. Salvaguardar la información también incluye el destruir la información correctamente.

Los siguientes pasos le servirán de guía para implementar un programa de seguridad que ayude a minimizar el riesgo de que la información sea expuesta.

Evalúe

Haga un inventario de acuerdo al tipo y ubicación de toda la información computarizada y archivos que tenga sobre sus clientes. Esto incluye la información personal que su empresa recibe de contratistas y otros mediante la red cibernética. Asegúrese de saber qué información delicada se encuentra almacenada en computadoras portátiles, en las computadoras personales de sus empleados, dispositivos con memoria flash (flash-drives), teléfonos celulares y asistentes digitales personales (PDA's).

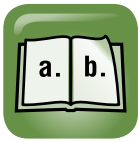
Como parte de la evaluación, fíjese en la efectividad de las salvaguardas de seguridad existentes para ver si hay algún riesgo de seguridad interno o externo previsibles en su red o en el software que emplea.

Proteja

Los documentos en papel que contienen información personal de identificación que pueden ser extraviados o robados hacen que usted sea más vulnerable a una violación de seguridad. La mejor manera de proteger documentos en papel, discos compactos, discos flexibles, unidades de discos zip, cintas y documentos de respaldo, es guardándolos bajo llave en un archivero o en una habitación con acceso limitado. Elabore un plan que explique y guíe a sus empleados acerca de los procedimientos para almacenar información delicada de una manera segura incluyendo la manera en la que los dispositivos pueden ser sacados de su área de trabajo. Verifique que toda la información delicada almacenada en computadoras personales esté codificada. Use software de cortafuegos para proteger su sistema computarizado contra ataques.

Reduzca

Si no tiene necesidad de cierta información personal de identificación, no la retenga. Si no es necesario o no existe un uso legítimo, no obtenga información delicada tal como números de Seguro Social de los consumidores. Si la información personal no cumple con una necesidad, diseñe un plan de retención de datos que indique qué información se debe retener, cómo protegerla, cuánto tiempo retenerla y cómo destruirla sin riesgo cuando no la necesite más.



Provea entrenamiento

Verifique que sus empleados sepan distinguir la información de identificación personal, la importancia de protegerla, las prácticas del programa y los procedimientos de seguridad de su empresa. La información personal incluye el nombre de un consumidor junto con un número de Seguro Social, el número de la licencia de conducir de Oregon o de la tarjeta de identificación de Oregon, el número de una tarjeta financiera, de crédito o débito y una contraseña que permitan que alguien tenga acceso a la cuenta financiera de un consumidor. Asimismo, enseñe a sus empleados los procedimientos de notificación si ocurre una falla en su sistema de seguridad.

Designe a uno o más empleados para propagar la información y coordinar el programa de seguridad.

Detecte

Evalúe regularmente los riesgos de seguridad poniendo a prueba y supervisando controles, sistemas y procedimientos clave. Además, fíjese si hay algún riesgo en su sistema de almacenamiento de información, ya sea un archivero que se cierra con llave o un sistema electrónico. Eso ayudará a responder rápidamente a ataques o intrusiones.

Al seleccionar proveedores de servicios externos, sepa su capacidad para mantener protección adecuada y requiera esa protección en su contrato con ellos.

Destruya

Proteja el acceso y el uso no autorizado a información de identificación que usted mantiene pero que ya no necesita destruyendola apropiadamente. Todos los datos electrónicos se deben borrar de tal manera que no se puedan leer o reconstruir.

La Legislatura de Oregon promulgó recientemente una ley para fomentar el reciclaje de dispositivos electrónicos, incluyendo computadoras de escritorio y portátiles. Ya que usted es responsable de salvaguardar la información identificación personal almacenada en cualquier equipo electrónico, usted debe destruir apropiadamente los archivos que contengan esta información, debe borrar o destruir el disco duro, o llegar a un acuerdo con la compañía de reciclaje que recoja los equipos computarizados para que destruya la información de manera adecuada antes de reciclar el equipo.

Más detalles en como proteger datos de identificación personal

Según la Ley de Oregon de Protección contra el robo de identidad, un programa de seguridad incluye lo siguiente:

Salvaguardas administrativas

- Designar a uno o más empleados para que coordinen el programa de seguridad.
- Identificar riesgos internos y externos razonablemente previsibles.
- Evaluar la suficiencia de las salvaguardas que se hayan puesto para controlar los riesgos identificados.
- Capacitar y conducir empleados en las prácticas y procedimientos del programa de seguridad.
- Elegir proveedores de servicios capaces de mantener salvaguardas apropiadas y requerir esas salvaguardas por contrato.
- Adaptar el programa de seguridad a cualquier cambio o nueva circunstancia en el negocio.

Salvaguardas técnicas

- Evaluar los riesgos en el diseño de la red y del software.
- Evaluar los riesgos en el procesamiento, la transmisión y el almacenamiento de información.
- Detectar, prevenir y responder a ataques a o fallos del sistema.
- Poner a prueba regularmente y supervisar la efectividad de los controles, los sistemas y los procedimientos clave.

Salvaguardas físicas

- Evaluar los riesgos de almacenamiento de la información y el método para destruirla.
- Detectar y prevenir intrusiones y responder a ellas.
- Proteger contra el acceso o uso de información personal no autorizado durante o después de la obtención, el transporte y la destrucción, de la información.
- Destruir información personal una vez que no sea necesaria para fines de negocios o si así lo requieren las leyes locales, estatales o federales, quemándola, pulverizándola, triturándola o modificando un archivo físico y destruyendo los medios electrónicos para que la información no se pueda leer ni reconstruir.

Nota: Toda persona, empresa, entidad gubernamental u organización que cumple y está sujeta a reglamentaciones o directivas de protección de datos adoptadas por la Ley Gramm-Leach-Bliley o la Ley de Portabilidad y Responsabilidad de Seguros de Salud (Health Insurance Portability and Accountability Act, HIPAA) no necesita elaborar procesos adicionales.
Sin embargo, deben seguir los requerimientos de Oregon para proteger la información personal de identificación de sus empleados.

Requerimientos para pequeñas empresas

Las empresas pequeñas, definidas así cuando pertenecen a la manufactura y cuentan con 200 empleados o menos, o de otro tipo si cuentan con 50 empleados o menos, cumplen con los requerimientos de protección si el programa de seguridad para desechar información contiene las salvaguardas administrativas, técnicas y físicas apropiadas para el tamaño y la complejidad de la empresa, así como para la índole y el alcance de sus actividades y la delicadeza de la información personal que mantiene.

Recursos adicionales

Comisión Federal de Comercio
www.ftc.gov/infosecurity

Estrategia Nacional del Departamento de Seguridad de la Patria para Proteger el Cibe-respacio
www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf

OnGuard en línea
www.OnGuardOnline.gov

Congelamiento de seguridad: Una opción para los consumidores

La Ley de Oregon de Protección contra el robo de identidad también proporciona a los consumidores una manera proactiva para proteger la información de identificación personal: el congelamiento de seguridad. Poner un congelamiento de seguridad en su historia de crédito es una manera efectiva de disuadir a los posibles ladrones de identidad.

Los residentes de Oregon pueden poner un congelamiento de seguridad en sus historiales de crédito mantenidos por una entidad de información crediticia, como Equifax, Experian o Trans-Union. Una vez activado el congelamiento, alguien que haya obtenido fraudulentamente información de identidad personal de otra persona no podrá obtener acceso al historial de crédito. El congelamiento también previene que prestamistas y otros obtengan acceso a su informe de crédito para examinarlo.

Nota importante: Tenga presente que un congelamiento de seguridad no prevendrá que un ladrón de identidad use indebidamente tarjetas y cuentas de crédito ya existentes.

Antes de decidir solicitar un congelamiento de sus archivos de crédito, considere si piensa hacer una compra que requiera que se examinen sus antecedentes de crédito. Por ejemplo, si piensa comprar un teléfono celular junto con el servicio, la empresa tendrá que tener acceso a su historial de crédito para finalizar la venta.

Obtención de un congelamiento de seguridad

Para congelar su crédito tiene que escribir a cada una de las tres entidades crediticias. Por ley, las entidades congelarán su archivo dentro de los cinco días laborables de haber recibido su pedido.

Costo

No hay ningún cargo si la persona es víctima de robo de identidad y reportó el robo de identidad a una entidad de cumplimiento de la ley. Para probar que informó a las autoridades, tiene que presentar una copia válida del reporte policial o del Formulario de Queja de Robo de Identidad de la Comisión Federal de Comercio.

Si no es una víctima de robo de identidad, igual puede poner un congelamiento de seguridad, pero tendrá que pagar una cargo. Cada entidad de información sobre crédito le cobrará $10. Por lo tanto, si pone un congelamiento en las tres entidades, pagará un total de $30.

Nota importante: Un congelamiento de seguridad no cubre a todos en una vivienda. Los cónyuges y compañeros deben congelar sus historiales de crédito por separado.

Acceso a su historial congelado

Si tiene un congelamiento de seguridad, algunas entidades gubernamentales y de cumplimiento de ley, así como las cortes y ciertas empresas privadas, pueden seguir teniendo acceso a su historial de crédito. Estas entidades incluyen empresas con las que está haciendo negocios, empresas a las que les debe dinero y agencias de colección.

Cómo "descongelar" el congelamiento

Los consumidores que ponen un congelamiento en su historial de crédito pueden quitar el congelamiento temporal o permanentemente o "descongelar" su historial para solicitar un nuevo crédito. Para hacerlo, siga los procedimientos en la carta de confirmación que le enviaron las entidades crediticias cuando puso su congelamiento de seguridad. Las entidades le pueden imponer un cargo máximo de $10 para quitar el congelamiento. Las entidades crediticias tienen que quitar el congelamiento dentro de los tres días laborables de haber recibido su pedido.

Para más detalles sobre los procedimientos para colocar y suspender un congelamiento de seguridad y ver modelos de cartas de pedido de congelamiento de seguridad, visite www.dfcs.oregon.gov y haga clic en Identity Theft (Robo de identidad).

Contacto:
503-378-4140
866-814-9710
www.dfcs.oregon.gov
Haga clic en Identity Theft (Robo de identidad)

440-4117s (4/08/COM) of 440-4117e (2/08/COM)