Cómo las empresas pequeñas pueden ayudar en la lucha contra el robo de identidad

El robo de identidad no solo es problema del consumidor. Es necesario que las empresas y los consumidores trabajen juntos para brindar la mayor protección posible contra el robo de identidad. Cuando la información personal de los clientes es robada, las empresas pueden no solo tener obligaciones legales para ayudar a corregir el problema, sino que también pueden sufrir pérdidas financieras.

Según el Better Business Bureau, las empresas pequeñas típicamente no están tan enfocadas en las seguridad de los datos como las corporaciones más grandes. Algunos propietarios de empresas pequeñas creen que cerrar su tienda con llave es suficiente protección contra el robo de datos importantes. Otros asumen que están mejor protegidos de lo que realmente lo están mientras otros sospechan que deberían estar haciendo más, pero no saben cómo.

Los registros de papel con información personal deben estar bajo llave y los terminales de computadora deben estar protegidas con contraseña.

La Comisión Federal de Comercio advierte a las empresas que bajo las enmiendas del 2003 a la Ley de Informes Imparciales de Crédito, 15 U.S.C. § 1681, las victimas de robo de identidad tienen derecho a obtener de las empresas una copia de la solicitud u otros registros de transacciones comerciales relacionados con su robo de identidad de manera gratuita. Las empresas también tienen que proporcionar estos registros a las autoridades que conducen la investigación.

Finalmente, las empresas que pierden la información de sus clientes, sin importar cómo ocurra la pérdida, pueden perder su activo más valioso, los clientes propios. Mientras más y más consumidores son víctimas de robo de identidad, toman su decisión de dónde hacer negocios dependiendo de qué garantías de protección de la privacidad ofrece la empresa. Por todas estas razones, las empresas ya no pueden ser

descuidadas con la protección de la información personal de sus clientes – y la suya.

Si no lo necesita, no lo recoja

Muchas empresas recopilan más información de la que necesitan, particularmente al pedir a los clientes que llenen formularios. Considere excluir la dirección, correo electrónico y número telefónico si solo necesita un nombre. El número de Seguro Social es un número confidencial que se requiere solamente si un cliente está generando ingresos (por empleo o inversión) para la declaración de impuestos – no debe ser recopilado en otros casos. Cuando ordene su siguiente colección de formularios, elimine toda la información que realmente no necesita.

La información personal no es para compartir

¿Pueden escuchar las personas esperando en fila en su oficina o tienda a otros dar a su personal sus números de teléfono o detalles de cuenta? Infórmele a los empleados que necesitan recopilar información personal de una manera discreta y silenciosa. Gire las pantallas de las computadoras para que no puedan ser vistas por nadie más que no sea el operador.

Proteja las tarjetas de clientes

Cuando los clientes están haciendo compras, asegúrese de que ellos tienen la privacidad suficiente para introducir con seguridad su número PIN. Coloque escudos en las terminales de punto-de-servicio y compruebe las terminales regularmente para verificar que el equipo no ha sido alterado. Ubique cameras de video de seguridad para que no puedan grabar la entrada de números PIN.

Sea inteligente con las tarjetas

El personal debe verificar que los clientes son quienes dicen ser comprobando las firmas en las tarjetas, y, si es apropiado, con el ID de foto. La Ley de Transacciones de Crédito Justas y Precisas, 15 U.S.C. Capítulo 41, requiere que los números de tarjeta de débito/crédito sean truncados al imprimir recibos electrónicamente (es decir, no imprima más que los últimos cinco números de la tarjeta) y que se borre la fecha de expiración de la tarjeta, para proteger mejor a los consumidores. No copie ningún número de la tarjeta que no necesita.

Si lo guarda, asegúrelo

Los registros de papel con información personal deben estar bajo llave, y los terminales de computadora protegidos por contraseña con contraseñas seguras. Coloque el servidor de la computadora en una ubicación segura y controlada, y mantenga otros dispositivos (como CDs de respaldo o unidades de cinta) bajo llave. Cierre con llave físicamente todas las laptops para prevenir que los ladrones se las lleven. Desarrolle e implemente políticas sobre quién puede llevar laptops a la casa, qué precauciones de seguridad se deben tomar cuando una laptop está fuera de la empresa (por ejemplo – no dejar una laptop en un carro, ya sea cerrado o no cerrado con llave), y qué acceso los empleados tienen a información mientras están fuera del sitio. También, desarrolle este mismo tipo de plan para los dispositivos móviles que puedan almacenar información personal o confidencial.

Mantenga a los clientes y otro personal no autorizado fuera de las áreas privadas y seguras.

Enseñe a los empleados a guardar datos en las unidades de red cuando estén disponibles y no en los discos duros "C:", que son mucho menos seguros. Si alguien roba el disco duro, la información almacenada en las unidades de red permanecerá protegida. Asegúrese de que su red y su computadora tienen el cortafuego más reciente, protección contra virus y malware y actualizaciones del sistema operativo. Esto ayuda a cerrar brechas de vulnerabilidad que se desarrollan mientras los hackers trabajan en nuevas maneras de obtener acceso. Proteja las redes de Wi-Fi asegurándose de que están cifradas y que el SSID (identificador de red) está oculto de transmisión por el enrutador o punto de acceso.

Considere un sistema de alarmas, preferiblemente uno que esté monitoreado por una compañía de seguridad. Su aseguradora de empresas podría asistirle con la evaluación de seguridad de sus operaciones.

Prevenga el fotocopiado no autorizado y coloque fotocopiadoras que se utilizan para copiar información sensible en un ambiente seguro, lejos del público. Ya que un número grande de fotocopiadoras más nuevas almacenan las páginas copiadas en un disco duro, asegúrese de que los datos sean asegurados o eliminados cuando la fotocopiadora es cambiada por otra o vendida a otro usuario.

Examine y entrene a los empleados

Un número significativo de robos de identidad empiezan con un empleado deshonesto que da información personal a un ladrón de identidad. Para proteger a su empresa contra el fraude interno, considere hacer verificaciones de antecedentes de los empleados que tienen acceso a información personal. Hay empresas que pueden hacer estas verificaciones (incluyendo antecedentes criminales, referencias y credenciales educativas) en su nombre. Considere llevar a cabo verificaciones regulares de autorización para empleados en áreas de alto riesgo (por ejemplo, con la evaluación del rendimiento anual de empleados) para asegurarse de que los empleados se mantienen libres de antecedentes criminales.

Asegúrese de que los empleados entienden las políticas de privacidad de información y cómo solicitar información personal a los clientes, tal como no pedir sus datos personales enfrente de otros, comprobar firmas, y mantener datos de clientes guardados bajo llave y en archivos informáticos protegidos con contraseña. Todos los desechos confidenciales, incluyendo información de tarjetas de crédito y documentos de identificación fotocopiados deben ser

triturados, preferiblemente con una trituradora de corte transversal, para evitar la búsqueda de basureros.

Si su información ha sido comprometida

Cree un plan de acción ahora para saber cómo responder a una filtración de datos. Si un ladrón de identidad ataca, o si alguna información se pierde, un plan de acción será invaluable para responder rápidamente frente a una filtración de datos. Tomar acción rápidamente puede ayudar a reducir daños potenciales, y puede ayudar a su empresa u organización a mantener su buena reputación y evitar responsabilidad en una acción civil.

Para responder a una filtración de datos o pérdida de información, usted tiene que seguir dos caminos al mismo tiempo: investigar el problema internamente y trazar un plan para notificar a las personas que un problema ha ocurrido. Determine qué información fue robada, cuándo y cómo sucedió, y qué tiene que hacer usted para asegurarse de que otros datos no sean robados o se pierdan.

Actuar rápido es esencial ya que la notificación inmediata puede ayudar a prevenir el robo de identidad o al menos mitigar el daño. Si un número pequeño de clientes son afectados, infórmelo por escrito de inmediato. Si un número más grande es afectado, usted querrá determinar un método más eficiente para aconsejar víctimas potenciales rápidamente.

También debe notificar a las autoridades de aplicación de la ley tan pronto como usted sea consciente de que la información se ha perdido o ha sido potencialmente comprometida.

La ley de Wisconsin sección 134.98 obliga a las empresas a notificar a individuales en ciertas circunstancias si su información personal se ha perdido, o si ha sido robada o comprometida de otra manera. Para más información sobre este tema, vea nuestra hoja informativa titulada "*Wisconsin's Data Breach Notification Law*."

Para obtener más información o para presentar una queja visite nuestro sitio web o contáctese con:

Wisconsin Department of Agriculture, Trade, and Consumer Protection
Bureau of Consumer Protection
2811 Agriculture Drive, PO Box 8911
Madison, WI 53708-8911

Correo electrónico: DATCPHotline@wi.gov
Sitio web: datcp.wi.gov
(800) 422-7128 TTY: (608) 224-5058

I:\dtcp\common\Fact Sheets\IDTheftSmallBusinessSPANISH908 (rev 4/23)