BUREAU OF CONSUMER PROTECTION Consumer Facts

Protecting Wisconsin Consumers for 75 Years

Como los negocios pequeños pueden ayudar en la lucha contra el robo de identidad

El robo de identidad no solo es un problema del consumidor. Se necesitan los negocios y consumidores trabajando juntos para brindar la mayor protección contra el robo de identidad. Cuando la información personal de sus clientes se roba, negocios pueden no solo tener obligaciones legales para ayudar a corregir el problema, sino también pueden estar sujetos a propias pérdidas financieras.

En acuerdo con el Better Business Bureau, negocios pequeños típicamente no están tan enfocados en seguridad de datos como corporaciones más grandes. Algunos propietarios de negocios pequeños creen que cerrando su tienda con llave es suficiente protección contra el robo de datos importantes. Otros asumen que están mejor protegidos de lo que realmente son mientras otros pueden sospechar que deberían estar haciendo más, pero no saben cómo.

La Comisión Federal de Comercio advierte a negocios que bajo las enmiendas del 2003 de la Ley de Informe Justo de Crédito 15 U.S. C. § 1681, victimas del robo de identidad tienen derecho a obtener de los negocios una copia de la solicitud u otros registros de transacciones comerciales relacionados con su robo de identidad de manera gratuita. Los negocios también tienen que proporcionar estos registros con una agencia investigadora de la ley.

Finalmente, los negocios que pierden la información de sus clientes, no importa como ocurra la pérdida, pueden perder su activo más valioso, los clientes propios. Mientras más y más consumidores llegan a ser víctimas del robo de identidad, toman su decisión de donde hacer negocios dependiendo de cuales garantías de protección de privacidad el negocio puede ofrecer. Por todas estas razones, negocios ya no pueden ser descuidados acerca de proteger la información personal de sus clientes-y su propio.

- **Si no lo necesite, no lo recoja**

  Muchos negocios recogen más información de lo 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 ganando ingresos (Empleo o inversión) para la declaración de impuestos – no debe recogerse de otra manera. Cuando ordene su siguiente colección de formularios, elimine toda la información que realmente no necesita.

- ## La información personal no es para transmisión

  ¿Pueden las personas esperando en fila en su oficina o tienda oír otros dar a su personal números de teléfono o detalles de la cuenta? Enseñe a los empleados que tienen que recoger información personal, hablar de una manera discreta y silenciosa. Gire pantallas de computadoras para que no puedan ser vistas por nadie más que el operador.

- ## Proteja tarjetas de clientes

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

- ## Sea inteligente de tarjeta

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

- ## Si lo guarda, asegúrelo

  Registros de papel con información personal deben bloquearse, y los terminales de computadora protegidos por contraseña con contraseñas seguras. Coloque el servidor de computadora en una ubicación segura y controlada, y mantenga otros dispositivos (ej. Hacer un respaldo de CDs o unidades de cinta) bloqueados. Cierra con llave físicamente todos los laptops para prevenir que los ladrones se alejen con uno. Desarrolle e implementa políticas sobre quien puede llevar laptops a la casa, cuales precauciones de seguridad se deben tomarse cuando un laptop esta fuera del negocio (ejemplo – no mantener un 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 tiempo de plan para dispositivos móviles que pueden almacenar información personal o confidencial.

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

  Enseñe a empleados a guardar datos en las unidades de red cuando estén disponibles y no en los discos duros "C:", cuales son mucho menos seguros. Si alguien roba el disco duro, información almacenada en unidades de red permanecerá protegida. Asegúrese de que su red y computadora tienen el cortafuego más reciente, protección de 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 redes de Wi-Fi asegurándose de que están cifrados y el SSID (identificador de conjunto de servicio) esta oculto de transmisión por el enrutador o punto de acceso.

  Considere un sistema de alarma, preferiblemente uno que este monitoreado por una compañía de seguridad. Su aseguradora de negocios podría atenderle con la evaluación de seguridad de sus operaciones.

  Prevenga el fotocopiado no autorizado y coloque fotocopiadoras que se utilizan para copiar información sensitiva en un ambiente seguro, lejos del público. Ya que un número grande de fotocopiadoras más actuales almacenan paginas copiadas en un disco duro, asegúrese de que los datos están seguros o eliminados cuando el copiadora esta comerciado con o vendido a otro usuario.

- ## Tamice y entrene empleados

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

  Asegúrese de que los empleados entiendan las políticas de privacidad de información y como solicitar información personal a los clientes, tal como no pedir sus datos personales enfrente de otros, comprobando firmas, y manteniendo datos de clientes guardado bajo llave y en archivos informáticas protegidos con contraseña. Todos los desechos confidenciales, incluyendo información de tarjeta de crédito y documentos de identificación fotocopiados deben que ser triturados, preferiblemente con una trituradora de corte transversal, para evitar la búsqueda de basureros.

- ## Si información se compromete

  Cree un plan de acción ahora para cómo responder a una violación de datos. Si un ladrón de identidad golpea, o si información se pierde, un plan de acción será invaluable en responder rápidamente a la violación de datos. Acción rápida puede ayudar a reducir daño potencial, y puede ayudar a su negocio o empresa mantener su buena reputación y evitar responsabilidad en una acción civil.

  Para responder a una violación 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 personas que un problema ha ocurrido. Determine cual información fue robada, cuando y como sucedió, y que usted tiene que hacer para asegurarse de que ningún otros datos están robados o perdidos.

  La sincronización es crítica 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 puede querer determinar un método más eficiente para aconsejar víctimas potenciales rápidamente.

  También usted debe notificar a agencias de aplicación de la ley tan pronto como usted esté consciente de que información se haya perdido o potencialmente ha sido comprometido.

  La ley de Wisconsin obliga Wis. Stat. s. 134.98 a los negocios notificar a individuales en ciertas circunstancias si su información personal se ha perdida, robada o comprometido de otra manera. Para más información sobre este tema, vea nuestra hoja informativa titulado “Wisconsin’s Data Breach Notification Law.”

Para más información, o para presentar una queja, visite nuestra página web o comuníquese con el Departamento de Protección al Consumidor.

Departamento de Protección al Consumidor
2811 Agriculture Drive
PO Box 8911
Madison WI 53708-8911

E-MAIL: DATCPWisconsinPrivacy@wi.gov

WEBSITE: datcp.wi.gov

(800) 422-7128

FAX: (608) 224-4677

TTY: (608) 224-5058