SEON

EBOOK

5 preguntas que hacerse al elegir una herramienta de prevención de fraude

SEON Technologies Ltd.
seon.io

info@seon.io
0044-20-351-44790

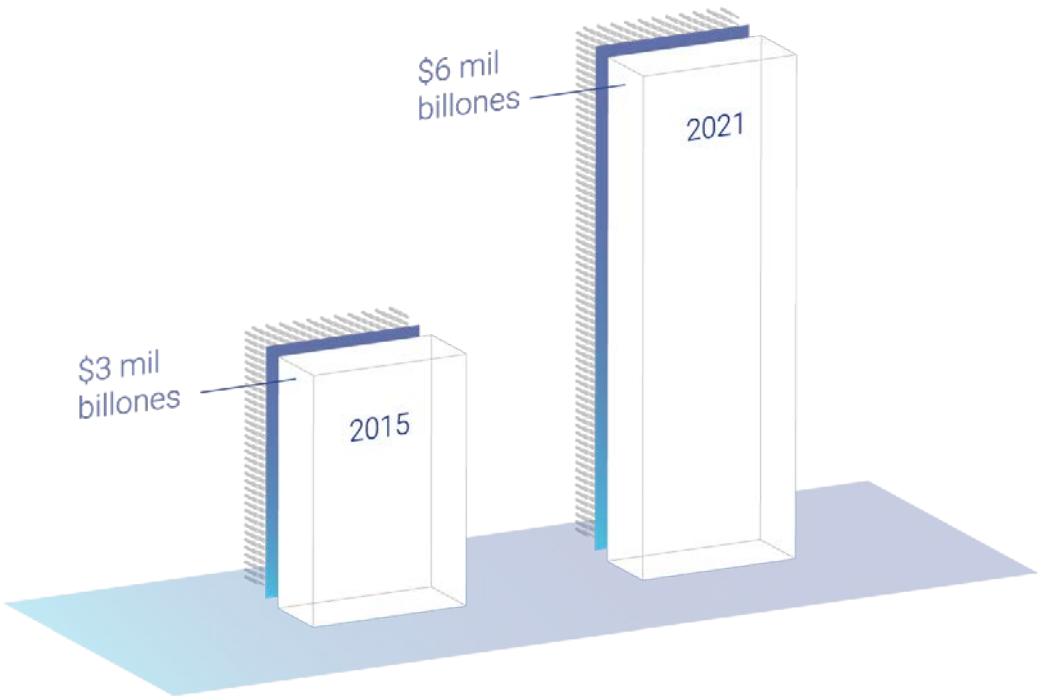
Tabla de contenidos

Introducción

Se estima que el mercado de detección de fraude alcanzará los 41 mil millones de dólares para 2022. Esto nos permite saber dos cosas. La primera es que veremos una explosión en el número de herramientas de prevención de fraude en los próximos años. Dos, si las compañías están gastando tales cantidades en ciberseguridad, ¿cuánto dinero están dispuestas a perder?

El costo del Cibercrimen en el mundo

Fuente: Cybersecurity Ventures Report 2017



Claramente, una cosa es cierta: la intensidad, escala y sofisticación de los ataques de fraude no muestra señales de disminuir. En este artículo, vamos a examinar algunos de los desafíos asociados con la detección de fraude, y te daremos toda la información que necesitas para encontrar una herramienta de prevención de fraude que haga sentido para tu negocio.

El fraude en línea:
El enemigo que cambia de forma

Sin importar tu industria, si operas en línea, puedes sufrir fraude. Ya sea que tu negocio esté en la industria de los viajes o las apuestas en línea, trabaje como un eCommerce o SaaS, nadie está a salvo.

Costo estimado del fraude en la industria de los viajes

Fuentes: (1) Reporte de Transacciones Digitales - Las agencias de viaje online como grandes objetivos de fraude (2) Amadeus.com - Arrojando luz sobre el fraude de tarjeta de crédito en las aerolíneas de canal indirecto

0.44 % Los vendedores de viajes pierden un promedio del 0.44% de sus ganancias por fraudes en línea (1)

4 % 4% de los boletos de avión son rechazados debido a sospechas de fraude (2)

25 % Algunos proveedores rechazan hasta un 25% de órdenes legítimas al carecer de datos de detección de fraude (2)

Además, los defraudadores y los negocios en línea juegan constantemente al gato y al ratón. Para los defraudadores, cada canal de pago nuevo es una oportunidad. Para los negocios, es difícil monitorear el sinfín de maneras en las que puede robarse la información. Actualmente, los principales abusos de fraude son:

- **compra con tarjeta de crédito robada:** los criminales roban números de tarjeta de crédito y los utilizan para comprar servicios o productos de tu compañía. Se emite entonces un contracargo, por el cual, tú como vendedor o institución financiera, puedes tener pérdidas;

- **robo de cuenta:** ataques más sofisticados que utilizan el robo de identidad (a menudo a través del phishing) para robar credenciales de una cuenta existente. La meta final, sin embargo, sigue siendo la misma: drenar dinero del usuario original;

- **cuentas falsas:** los defraudadores falsifican información o utilizan identificaciones robadas para crear una cuenta nueva. Una política de registro laxa puede permitir la incorporación de más cuentas, pero también puede abrirle la puerta a agentes maliciosos. Esto fue lo que pasó en el escándalo de Wells Fargo, donde el banco descubrió más de 3 millones de cuentas falsas en su base de usuarios;

- **abuso de cuentas:** los defraudadores utilizan cuentas vinculadas para abusar de los términos del vendedor, ya sea para beneficiarse de promociones de ingreso o recompensas de lealtad;

- **fraude amistoso:** el único punto de esta lista que es resultado de un error honesto. Los usuarios o clientes a veces se confunden o se distraen, realizan una compra inusual, y después solicitan un contracargo.

Los principales desafíos de la prevención de fraude

Conocer al enemigo es una cosa. Colocar barreras en su camino es otra. Hasta la fecha, hay tres desafíos principales que los negocios deben enfrentar cuando evalúan herramientas de prevención de fraude.

2.1 UNA TALLA NO LE QUEDA A TODOS

El fraude en un sitio para reservar hoteles será completamente diferente al de una boutique en línea. Esto significa que las herramientas de prevención de fraude son demasiado de nicho o muy generales para cubrir las necesidades específicas de la industria.

2.2 PATRONES DE ATAQUE EN EVOLUCIÓN

Los defraudadores se adaptan constantemente. Si un vector de ataque es bloqueado frecuentemente, pasarán a usar otra técnica. ¿La herramienta de prevención de fraude es flexible y capaz de evolucionar con el tiempo? O solamente te protege de un tipo de ataque.

2.3 OFRECER UNA EXPERIENCIA DE USUARIO SIN INCONVENIENTES

Los clientes son cada vez más demandantes cuando se trata de experiencia de usuario. Esto es particularmente cierto al inscribirse a un nuevo servicio o procesar una transacción. ¿Toma demasiado tiempo debido a tus revisiones de seguridad? Podrías ver cómo tus tasas de rebote y abandono de carritos aumentan drásticamente.

2.4 ENTREGAR RESULTADOS EN TIEMPO REAL

Las revisiones manuales deberían ser el último recurso. Sabemos que alenta los procesos, y como vimos anteriormente, esto puede impactar negativamente en tu negocio. Del mismo modo, tu herramienta de prevención de fraude no puede desperdiciar el tiempo. Entre más larga sea la espera, más datos puedes agregar. Pero esto puede significar un sacrificio de la tasa de conversión en pro de la seguridad.

2.5 PERMANECER EN CUMPLIMIENTO

Añadido al desafío de la prevención de fraude, aquellos que quieren prevenir los ataques deben cumplir con cada vez más reglas y regulaciones. Esto es particularmente cierto para las leyes de protección de datos (como el Reglamento General de Protección de Datos (GDPR) (Regulación (UE) 2016/679), y las regulaciones que gobiernan las transacciones financieras (tal como el PSD2 de la UE).

Principales sistemas de prevención de fraude
Un repaso

Conforme aumentan los ataques de fraude alrededor del mundo, costando a las industrias miles de millones de dólares por año, también lo hacen las herramientas de prevención de fraude. Desafortunadamente, no todas se crean de la misma manera. En la siguiente sección, daremos un rápido repaso de varias de las soluciones y consideraremos sus pros y sus contras.

3.1 SOLUCIONES API DE NICHO

Incluye: Emailage, Perseuss, Whitepages Pro

Estas soluciones se enfocan en agregar datos de diversas fuentes, y compartirlos para obtener una perspectiva de quiénes podrían ser los defraudadores. La idea es dar a los vendedores fuerza en los números, al permitirles incorporar información en una gran base de datos.

Mientras que esta solución da buenos resultados, existen dos desventajas principales. La primera es que necesitas una licencia por cada proveedor, las cuales pueden acumularse rápidamente. La segunda es que se necesita desarrollar una plataforma middleware, lo que puede añadir costos de desarrollo y complejidad en la integración.

3.2 PLATAFORMAS TRADICIONALES HEREDADAS

Incluye: Kount, Threatmetrix, CyberSource

La prevención de fraude no es nada nuevo y los servicios como los que mencionamos anteriormente han estado en operación por muchos años. También intercambian datos entre empresas para predecir dónde podrían aparecer los defraudadores a continuación, y enfocarse en la gestión de pagos para vendedores más grandes en el mundo.

Uno de los inconvenientes es que lo que gana estas soluciones en antigüedad, lo pierden en términos de agilidad y asequibilidad. Las ofertas son por lo general costosas, y la tecnología es anticuada lo que hace que la integración a nuevas plataformas sea menos intuitiva que con otras soluciones. Además, estas compañías despliegan nuevas características en un ciclo más lento, lo que puede dañar la ventaja competitiva de tu compañía.

3.3 SOLUCIONES INTERNAS

Reclutar tu propio departamento de prevención de fraude es absolutamente posible si ya tienes un presupuesto destinado a las TI y al desarrollo. Estos son preferidos por razones de privacidad de datos, y el equipo se beneficiará de un gran conocimiento del producto o servicio, lo que debería simplificar los procesos de implementación.

Sin embargo, el principal problema es la escalabilidad. Los salarios y los costos no son fáciles de presupuestar cuando nunca sabes qué tan frecuentes serán los ataques de fraude. Sí solo incrementan en un mes del año, ¿puedes de

pronto contratar a más gente? Además, puede ser difícil monitorear los gastos, mientras que las soluciones de terceros tendrán cantidades claras de retorno de inversión y resultados transparentes.

3.4 SOLUCIONES BASADAS EN LA NUBE

Incluye: SEON, Sift Science, Riskified

Las soluciones basadas en la nube de proveedores independientes tienen numerosas ventajas. Sus posibilidades de escalabilidad es una de las más obvias, ya que puedes pagar dependiendo del uso. Esto, por supuesto, tiene una gran influencia en los costos y en reducir los gastos misceláneos. De manera similar, el proveedor se encarga de las actualizaciones y las resoluciones de bugs. No hay necesidad de monitorear mejoras o desarrollar internamente características adicionales.

Es importante notar que varios proveedores de servicios de pago incluyen la prevención de fraude basada en la nube como la característica básica para los vendedores.

BlueSnap, Braintree, Chase Paymentech, GoECart, Magento y X-Cart lo ofrecen como parte de sus paquetes, y aunque te puedas beneficiar de no tener que integrar una solución adicional, estas herramientas pueden carecer de características de transparencia.

Seleccionar las características basadas en la nube correctas

Como vimos anteriormente, las soluciones basadas en la nube permiten amplia agilidad y flexibilidad que le permite a los negocios crecer con completa calma. Para los otros beneficios, es importante hacer las preguntas correctas. La siguiente selección debería encaminarte hacia la solución perfecta.

4.1 FLEXIBILIDAD CON CAMPOS Y PARÁMETROS DE DATOS

Entre más precisos sean los datos con los que puedas alimentar a los sistemas, más precisos serán los resultados. Comúnmente, estos datos se adquieren a través de campos que los usuarios pueden completar con información personal. Por ejemplo, correo electrónico, dirección IP, cantidad y divisa de la transacción, todos estos pueden ser factores de riesgo sólidos.

Sin embargo, los operadores de billeteras electrónicas (los casinos y mercados en línea) tienen necesidades muy distintas a las de los vendedores en línea. Para adaptarse a necesidades específicas de la industria, el proveedor debería ofrecer la capacidad de procesar campos y parámetros personalizados. Idealmente, las solicitudes específicas del vendedor se manejan fácilmente, y sin cargos adicionales.

Finalmente, agregar campos personalizados pierde sentido si el motor no sabe cómo considerarlos en la creación de reglas. Un ejemplo clásico es que los defraudadores típicamente compran zapatos de talla 9 en línea ya que son más fáciles de revender. ¿Tu solución podría incorporar este conocimiento en su modelo de reglas de decisión?

4.2 LA VELOCIDAD LO ES TODO

La precisión es una cosa, la velocidad es otra métrica sumamente importante. Una vez integrada en tu plataforma, ¿qué tan rápido puedes tomar una decisión para permitir los procesos? Idealmente, tu herramienta de prevención de fraude debería ofrecer bloqueo en tiempo real y un tiempo corto de respuesta.

El sistema también debería procesar solicitudes asíncronas, donde uno de los puntos de datos se verifica inmediatamente, mientras que los otros se enfilan para ser analizados sin retrasar la experiencia de cliente.

4.3 PUNTUACIÓN DE RIESGO TRANSPARENTE Y AJUSTABLE

Los sistemas de detección de fraude entregan resultados a través de la puntuación o la clasificación. El primero te da una mejor perspectiva de cuánta confianza puedes depositar en cada usuario. Con las clasificaciones, únicamente obtienes un sí o un no, lo que puede ser particularmente problemático si la solución no es completamente whitebox.

Sin embargo, ambos métodos pueden ser confusos si tu herramienta carece de la capacidad de afinar el modelo de puntuación o clasificación. Siempre es

mejor preguntar al proveedor desde antes si los ajustes manuales están disponibles, y cómo se llevan a cabo.

4.4 SOLUCIONES WHITEBOX VS BLACKBOX

Que la solución sea whitebox o blackbox simplemente describe cuánta transparencia obtienes como usuario. Las soluciones blackbox no van más allá para explicar su decisión, lo que las vuelve más difíciles de afinar. Las soluciones whitebox, por otro lado, darán explicaciones claras en forma de árboles de decisiones o traducciones legibles para los humanos o del razonamiento del sistema.

4.5 INTEGRACIÓN Y SOPORTE SIN INCONVENIENTES

Tus desarrolladores o CTO deberían verificar por adelantado la documentación API. Tener un entendimiento claro de cómo se integrará la herramienta con tu plataforma te ahorrará horas de costosas dificultades técnicas a largo plazo. Algunos puntos a considerar:

- Número de extremos de integración
- Número de campos de datos a procesar
- ¿La integración incluye soporte y capacitación?

Integrar una herramienta de prevención de fraude puede ser temporalmente disruptivo para tu negocio. Nuevamente, un conocimiento claro del proceso previo a la integración traerá más recompensas a largo plazo.

4.6 ENRIQUECIMIENTO DE DATOS

Analizar los datos es bueno. Enriquecerlos con fuentes adicionales es incluso mejor. Simplemente, entre más datos obtengas acerca de una transacción o identificación de usuario, más precisos serán los resultados. Es por ello que es importante recolectar información de tus campos de datos seleccionados, pero también observar cosas que no le puedes preguntar al usuario, tales como

- **Dirección IP:** y no solo la geolocalización, que los defraudadores son expertos en falsificar hoy en día. Debería revisar el tipo de ISP, detección de proxys, puertos abiertos, etc…

- **Análisis de correo electrónico:** para obtener información acerca del tipo de dominio (gratuito/personalizado/desechable), fecha de creación, existencia de redes sociales, etc…

- **Dirección:** primero, validándola, y después recolectando información adicional como el tipo de dirección (oficina, residencial, comercial).

- **Número de teléfono:** revisar su validez, pero también el tipo (línea fija o celular). Vinculándola con el nombre del propietario real, número de Google Voice o Skype también puede revelar una imagen más clara.

- **Comportamiento en línea:** ¿el sistema puede obtener información tal como el tiempo en el sitio, mapa de calor de clics o historial del navegador?

- **Base de datos de números BIN:** tal como el banco emisor, país, tipo, etc…

4.7 USABILIDAD DE INTERFAZ GRÁFICA DE USUARIO Y EXPERIENCIA DE USUARIO

Una característica que a menudo se pasa por alto en las soluciones de prevención de fraude es su facilidad de uso. Los mejores ingenieros no siempre son los mejores diseñadores de experiencia de usuario, razón por la cual algunas interfaces pueden ser confusas, sobrecargadas y frustrantes.

Aunque la navegación es una preferencia personal, los usuarios deberían considerar si las siguientes características están disponibles para hacer su vida más fácil a largo plazo:

- **Función de búsqueda:** ¿está disponible y puedes encontrar transacciones específicas? Para los usuarios avanzados, ¿puedes encontrarlas con base en parámetros personalizados y reemplazar las consultas SQL?

- **Función de bitácora:** los analistas de datos no deberían verificar la misma transacción dos veces, así que la bitácora es importante.

- **Creación de flujos de trabajo:** ¿puedes crear filtros de búsqueda específicos para usarlos más adelante?

- **Presentación de datos flexible:** ¿puedes ver las cuentas conectadas de los usuarios? ¿Puedes enlistar las transacciones en el orden que quieras? ¿Puedes ver todo el historial de transacciones de un usuario?

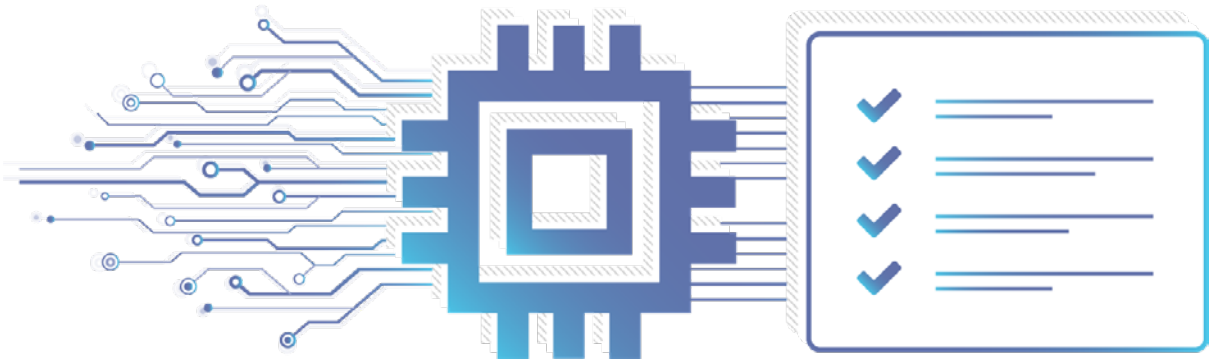
- **Reportes:** ¿puedes obtener datos claros de detección de fraude? ¿Están dispuestos en una forma que es entendible para tu equipo?

- **Motor de reglas personalizadas:** ¿qué tan fácilmente puedes ajustar las reglas para mejorar la toma de decisiones? ¿Necesitas apoyo del proveedor o puedes entrenar a tu personal para que lo haga? ¿Puedes crear reglas de velocidad o validar la efectividad de las reglas con una matriz de confusión?

4.8 LOS BENEFICIOS DEL MACHINE-LEARNING

Cualquier herramienta de prevención de fraude que se respete debería mejorar su precisión con el tiempo. Mientras que algunos sistemas hacen uso de algoritmos, no todos son de machine-learning. La ventaja de esta tecnología es que la inteligencia artificial puede actualizarse con base en la tasa de éxito.

Y es importante notar que ciertos proveedores, como SEON, creen que el machine learning es más eficiente al combinar la IA con la participación humana para mejorar y afinar su predicción. Entre más uses este motor único, menos ataques fraudulentos dañarán a tu compañía.



4.9 MODELO DE PRECIOS

Para la mayoría de los negocios en línea, los márgenes son muy bajos, y la competencia es feroz. Por lo tanto un modelo de precios razonable para tu herramienta de prevención de fraude es tan importante como sus características. A continuación hay algunos puntos a considerar antes de seleccionar a tu proveedor:

- **Cargos mensuales o modelo de suscripción:** bueno para calcular tus gastos anuales. Sin embargo, ten en cuenta que los proveedores pueden colocarte en un nivel de precios que no es conveniente para ti. Además, la escalabilidad es reducida, ya que debes continuar pagando incluso si tus ventas caen en temporadas.

- **Microcargos con base en llamadas API:** un modelo interesante que es tanto flexible como adaptable. Es más fácil obtener una perspectiva clara de tus costos, y predecir el presupuesto si tus transacciones fluctúan regularmente.

- **Porcentaje de la transacción verificada:** fácil de entender, pero a menudo más costoso que otros modelos anteriores. Algunos proveedores ofrecen una garantía de contracargos con base en este modelo, desafortunadamente, esto usualmente incrementa la tasa de falsos positivos.

4.10 COSTOS ADICIONALES

Además de un modelo de precios adecuado, también deberías considerar si el proveedor tiene:

- **Un costo de integración:** no es ideal porque significa que debes pagar por adelantado sin ninguna validación de precisión.

- **Cargos de soporte:** otro costo oculto que hay que tener en cuenta.

- **Una prueba gratuita:** idealmente, el proveedor debería tener la suficiente confianza en la capacidad de su herramienta como para dejarte probarla gratis. Debería venir en forma de una prueba A/B clara para que puedas comprar su solución con completa tranquilidad.

Y recuerda que, en última instancia, no vale la pena implementar una herramienta de prevención de fraude si los costos sobrepasan tus pérdidas por fraude. Comprar una solución puede ser costoso, y esto es sin considerar el tiempo y recursos que se pierden con la implementación, la rotación de clientes debido a falsos positivos o incluso la capacitación de personal.

4.11 MONITOREAR LA EFICIENCIA Y MEJORAS

Finalmente, no es suficiente integrar una solución y dejar que corra por sí sola. La herramienta de prevención de fraude debería proporcionar suficientes reportes y analíticas para ti y tu equipo para monitorear su eficiencia. Los procesos manuales, la detección de precisión (verificada a través de matrices de confusión) y los retornos de inversión son mejoras que debes revisar regularmente. En última instancia, una solución que no reduce las pérdidas o mejora el punto de partida no es una con la que quieras estar estancado a largo plazo.

Conclusión

Con un número creciente de herramientas de prevención de fraude disponibles en el mercado, los vendedores pueden confundirse fácilmente. Ya es malo de por sí que las compañías tengan que lidiar con incesantes ataques de fraude como para que además tengan que enfrentar desafíos al elegir la solución correcta.

Esperamos que este ebook sirva como una buena introducción. Ahora deberías tener una idea más clara de qué herramientas hacen sentido para tu compañía. Y recuerda mantenerte informado, ya sea sobre las últimas técnicas de ataque o herramientas de ciberseguridad, siempre es la mejor forma de estar un paso al frente de los defraudadores y de la competencia.

Para más información sobre SEON, visite nuestro sitio web:

www.seon.io

O programa ahora una llamada de presentación de productos personalizada.

Programa una llamada

SEON

SEON Technologies Ltd.
seon.io

info@seon.io
+44 20 8089 2900