SEON

Incorporación digital: cómo funciona, herramientas y soluciones

SEON Technologies Ltd.
seon.io

info@seon.io
+44 20 8089 2900

Tabla de Contenidos

Para las compañías en línea, no hay nada más importante que el proceso de incorporación de usuarios.

Tú gastas enormes cantidades de dinero en atraer usuarios a tu sitio, con muchos negocios con departamentos enteros dedicados a optimizar ese sitio para que el tráfico se convierta en usuarios.

Obviamente, las compañías quieren que la incorporación sea **tan rápida y con menos fricción** como sea posible, mientras se cumplen con las regulaciones en su industria y mercado, y nada podría estar más alejado de la verdad, la fase de incorporación es crucial no sólo para la experiencia de usuario sino por razones de fraude y riesgo.

En el papel, un modelo de negocios completamente en línea tiene enormes ventajas. Puedes apuntar a un mercado global, operar 24/7 y tener más control de los datos. Pero hay un área donde el modelo de venta en mostrador tradicional gana: verificar la identidad de las personas. Este es exactamente el desafío del proceso de incorporación de clientes digital moderno.

Veamos por qué funciona, cuándo es riesgoso y cómo hacerlo de la forma más fluida posible sin atraer a los defraudadores.

¿Qué es la incorporación digital?

La incorporación digital de clientes es el proceso a través del cual los negocios incorporan o adquieren nuevos usuarios en línea. Puede llevarse a cabo en sitios web o dentro de una aplicación, pero, crucialmente, no en una sucursal o tienda, ya que es digital.

Dado que el personal no interactúa con estos usuarios en persona, es vital establecer procedimientos de seguridad para asegurar que los usuarios son realmente quienes dicen ser.

Con el aumento en los smartphones con cámaras de buena calidad, nos hemos acostumbrado a tomar selfies o proporcionar fotos de nuestros documentos de identificación durante la incorporación. Mientras que en los servicios financieros esto es esperado y obligatorio, en otras áreas puede considerarse como demasiado. Tus usuarios están ansiosos por usar tu servicio, pero no necesariamente te confiarán sus detalles sensibles.

De lo que hablamos es de la identificación biométrica, una forma del KYC duro. Duro porque históricamente es duro de vencer, y también porque añade una gran cantidad de fricción a tus usuarios.

¿Cómo funciona el proceso de incorporación digital de clientes?

La incorporación digital es una forma de adquirir clientes que sucede completamente en línea. El usuario simplemente se registra a tu servicio utilizando su dispositivo, proporcionando los detalles necesarios paso por paso. El flujo de incorporación no solo sirve para conocer a tu cliente (KYC) y los estándares de cumplimiento de la diligencia debida de cliente (CDD).

En su forma más simple, la incorporación digital te permite convertir tus visitantes en usuarios de servicio o clientes a cambio de que te proporcionen sus detalles personales al registrarse, lo que te permite verificar su identidad.

¿Quién usa la incorporación digital?

La incorporación digital puede usarse por cualquier negocio que desee atender clientes en línea, pero es absolutamente esencial para los vendedores en línea e instituciones financieras que operan exclusivamente en línea, quienes no tienen otra manera de registrar usuarios. También se usa en la incorporación de empleados para gestionar a trabajadores remotos, para ahorrar tiempo en papeleo y/o gestionar digitalmente los datos de empleado.

Los desafíos de la incorporación digital

Es preciso decir que los negocios que desean permanecer en el camino correcto de la ley no son recompensados por sus esfuerzos. Frecuentemente, los clientes que encuentran demasiados obstáculos durante el proceso de registro lo abandonan.

Esto se conoce como **rotación de clientes** y es un campo de batalla cada vez más grande en la nueva ola de modelos de negocio en línea.

Como la economía de siempre en línea no muestra signos de disminuir, los clientes esperan ser capaces de inscribirse a nuevos servicios de la manera más fácil posible. Añadir demasiados pasos de verificación se convierte en un obstáculo que los envía con competidores más laxos. Sin embargo, la legislación y las mejores prácticas de seguridad requieren precaución.

El software KYC es típicamente costoso

Para empeorar las cosas, las compañías que confían en servicios de KYC tradicionales encuentran que su dinero se esfuma rápidamente, ya que el costo de verificación de cada cliente oscila entre los **10 y 100 dólares**.

Incluso las soluciones alternativas de incorporación digital que se enfocan en la identificación, tales como Stripe Identity, sólo reducen el costo a **$1.5 por verificación KYC,** lo cual sigue siendo costoso si tienes un gran volumen de solicitudes. Especialmente si la mayoría de ellos son fraudulentos. Estás esencialmente gastando verificaciones en usuarios inválidos que no aportan nada a tu negocio.

Las identificaciones son fáciles de falsificar

Los defraudadores hacen su mejor esfuerzo para vincular identidades de la vida real con cuentas en línea. Por eso roban las identidades de otras personas o crean identidades sintéticas al combinar datos reales y falsos.

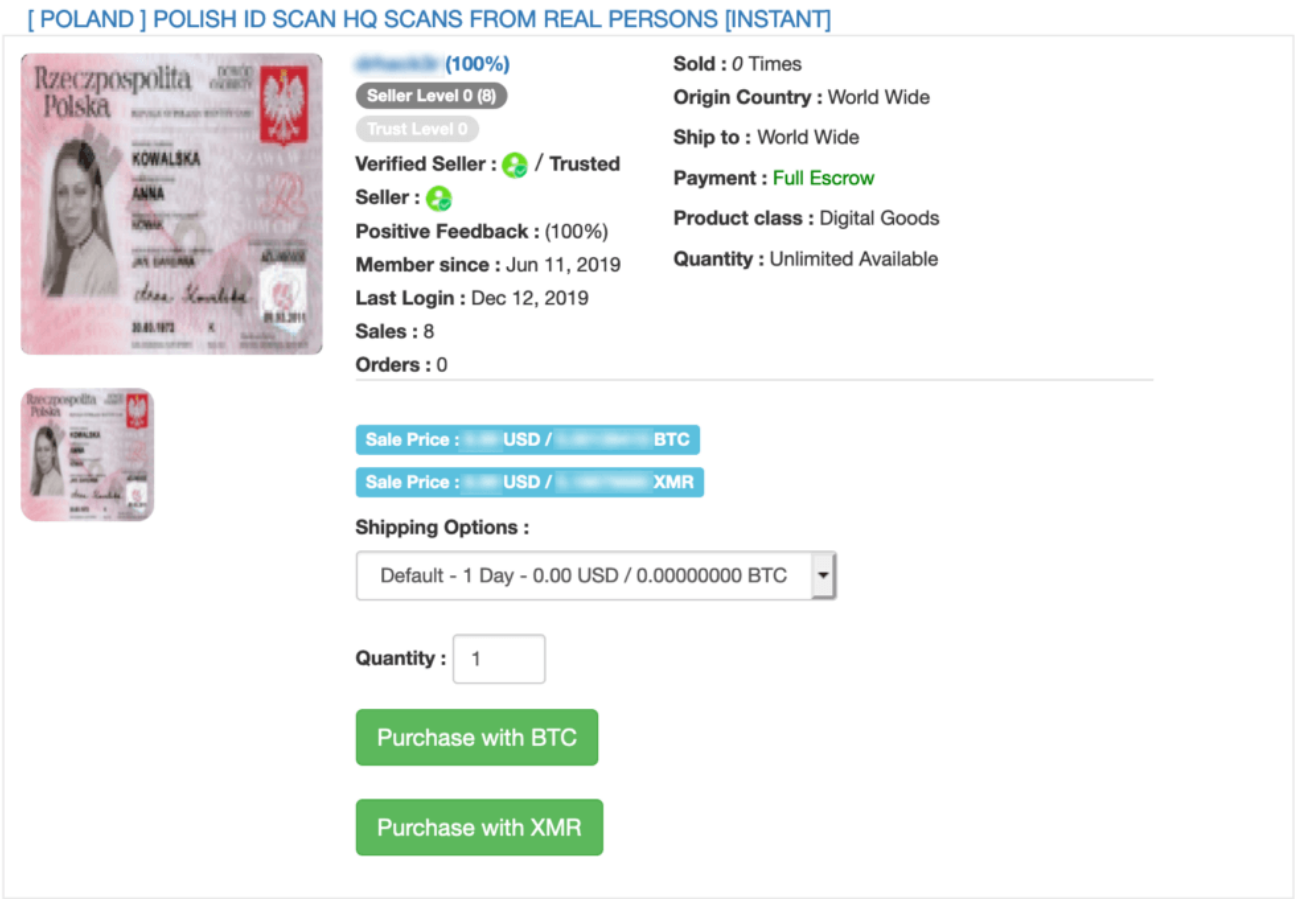
Tradicionalmente, sólo las compañías que necesitan verificar las identidades de las personas eran las instituciones financieras ya que fracasar en identificar que alguien incurre en riesgo significa que pueden terminar prestando dinero a criminales que utilizan datos falsos o robados y que están listos para desaparecer sin pagar.

Pero ya que la mayoría de las compañías que ofrecen pagos se han transferido en línea, los defraudadores han establecido nuevos métodos para vencer las verificaciones de identidad. Usarán correos y números de teléfono desechables o recién creados al registrarse en diferentes servicios, lo que les permite usarlos como trampolín para otros esquemas.

Las biométricas son fáciles de superar

Para superar verificaciones de incorporación digital, los defraudadores:

- **usarán información robada,** adquirida mediante el phishing o compradas en mercados de la darknet en forma de "fullz", paquetes que incluyen el nombre, dirección y número de tarjeta de crédto de alguien;
- **crearán documentos de identificación** (utilizando Photoshop u otro software de edición;
- **combinarán datos reales y falsos para crear identificaciones sintéticas.**



Ejemplo de escaneo de una tarjeta de identidad real que puede ser utilizada para el robo de identidad

También está ocurriendo un incremento en el servicio de renta de identificaciones. Esto es cuando alguien vende sus documentos de identidad voluntariamente a criminales que las necesitan para cometer sus crímenes. Al permitir que los defraudadores utilicen su identidad en línea, la persona se vuelve un cómplice y recibe una pequeña comisión.

Los detalles de identificación de todos son valiosos. Los defraudadores a menudo usan los detalles de identidad de personas fallecidas e incluso niños porque estos últimos tienen puntajes de crédito positivos de forma predeterminada.

Además, la popularidad creciente de la tecnología basada en IA, tal como los deepfakes, que permiten a los criminales crear videos falsificados o grabaciones de audio de personas sin su permiso, generan dudas respecto a la relevancia de autenticación basada en identificación.

Aunque esto pueda parecer ciencia ficción, se ha demostrado de forma preocupante que la tecnología biométrica es relativamente fácil de superar, incluso con métodos de baja tecnología.

Por ejemplo, Kraken Security Labs ha demostrado que se pueden falsificar las huellas dactilares de cualquier persona por menos de 5 dólares, simplemente utilizando una foto de sus dedos en primer plano. El reconocimiento facial automatizado puede superarse imprimiendo una foto del individuo, según Naked Security.

¿La conclusión? La biometría es buena para la identificación, pero tiene su propio riesgo desde un punto de vista de la seguridad.

Cómo establecer un proceso de incorporación digital para la detección de fraude

El proceso de incorporación digital se está volviendo rápidamente un campo de batalla importante para las compañías en línea. Maximizar la tracción con altas tasas de aceptación es clave. Si la gente no puede registrarse lo suficientemente fácil y rápido, se irán con los competidores.

Entonces, ¿cómo luce una experiencia de incorporación sin fricción? Tiene que tener todo lo siguiente.

> **Fácil:** nadie quiere rellenar largos formularios y responder cuestionarios exhaustivos para acceder a un nuevo servicio hoy en día, ya sea una tienda en línea o para aplicar para una nueva tarjeta de débito.

> **Fácil:** sin largos retrasos para aceptar una solicitud. Esto significa tener un entendimiento claro de los pasos requeridos y dar expectativa de cuánto debería tomar todo el proceso.

> **Sin inconvenientes:** las medidas de seguridad largas pueden alejar a nuevos clientes al crear rotación. Pedirle a los clientes que proporcionen documentos adicionales o una selfie, o incluso tener una conversación por videollamada para completar la incorporación puede ser una barrera para aquellos que desean ingresar rápidamente en una cuenta de banco.

Sea cual sea tu flujo de incorporación de cliente, estarás capturando mucha información acerca de tu usuario en cada paso.

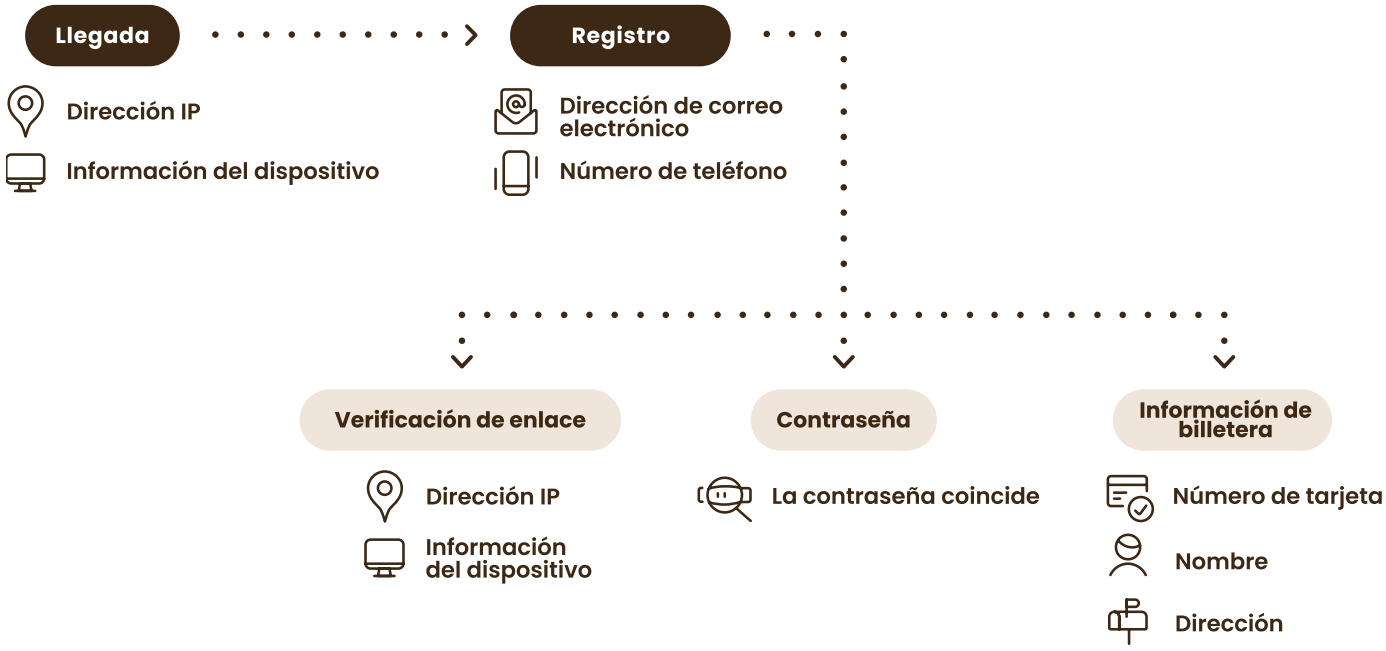
En lugar de forzar a todos tus usuarios a callejones sin salida de KYC duro obligatorio y depender de un costoso servicio de verificación independiente, **puedes utilizar los datos que proporciona para conformar tus propios perfiles de usuario.**

Lo que es más, puedes aplicar puntuaciones de riesgo en cada paso para evaluar si permitir o no al usuario continuar. Si se determina que es riesgoso, puedes disparar una verificación de seguridad más estricta o una revisión manual. Si se determina que es una amenaza, puedes bloquearlo completamente, o cualquier combinación de los anteriores.

Este enfoque se conoce como **fricción dinámica,** y es el pan de cada día para muchos de nuestros clientes.

Piensa en tu experiencia de usuario típica durante el registro. Idealmente, los usuarios deberían revelar gradualmente más y más sobre ellos en un juego de establecer confianza mutua.

1. Cuando lleguen a tu sitio web o aplicación, verás su **IP** e **información del dispositivo.**
2. Cuando se inscriben o registren te proporcionarán su medio de contacto; **una dirección de correo electrónico o número de teléfono.**
3. Tú enviarás un enlace de activación, el cual pueden utilizar **desde un dispositivo diferente** del cual también te enteras.
4. Puedes solicitarles que proporcionen una **contraseña.**
5. Y finalmente, solicitas que proporcionen su **número de tarjeta, nombre y/o dirección.**



Esta lista de verificación será más o menos la misma a lo largo de los distintos verticales, con la omisión de algunos detalles en ciertas industrias. Pero el punto es que **la verificación de riesgo de cada uno de esos detalles** en el paso en el que los recibes debería darte una vista clara de con quién estás tratando, lo que te permite satisfacer los requerimientos de diligencia debida del cliente incluso antes de solicitar una selfie o una identificación.

Soluciones de incorporación digital

Entonces, ¿cómo puede un negocio obtener una mejor idea de a quién están incorporando sin sacrificar la experiencia de usuario, el costo y la seguridad? En SEON, creemos que necesitas un triple enfoque para la incorporación digital:

1. KYC

Las herramientas electrónicas know your customer (eKYC) han mejorado en la sofisticación y la facilidad de uso en años recientes. Ahora puedes integrarlas directamente en tu plataforma y enviar y recibir datos a través de llamadas API. En la mayoría de los casos, necesitarás enviar:

- **un nombre completo;**
- **una digitalización de un documento de identificación oficial.**

La herramienta en línea de KYC realizará entonces una revisión en tiempo real para comprobar que el nombre y las identificaciones coincidan con registros existentes, o al menos te da una idea de qué tan riesgosa luce esa incorporación con base en sus propios parámetros.

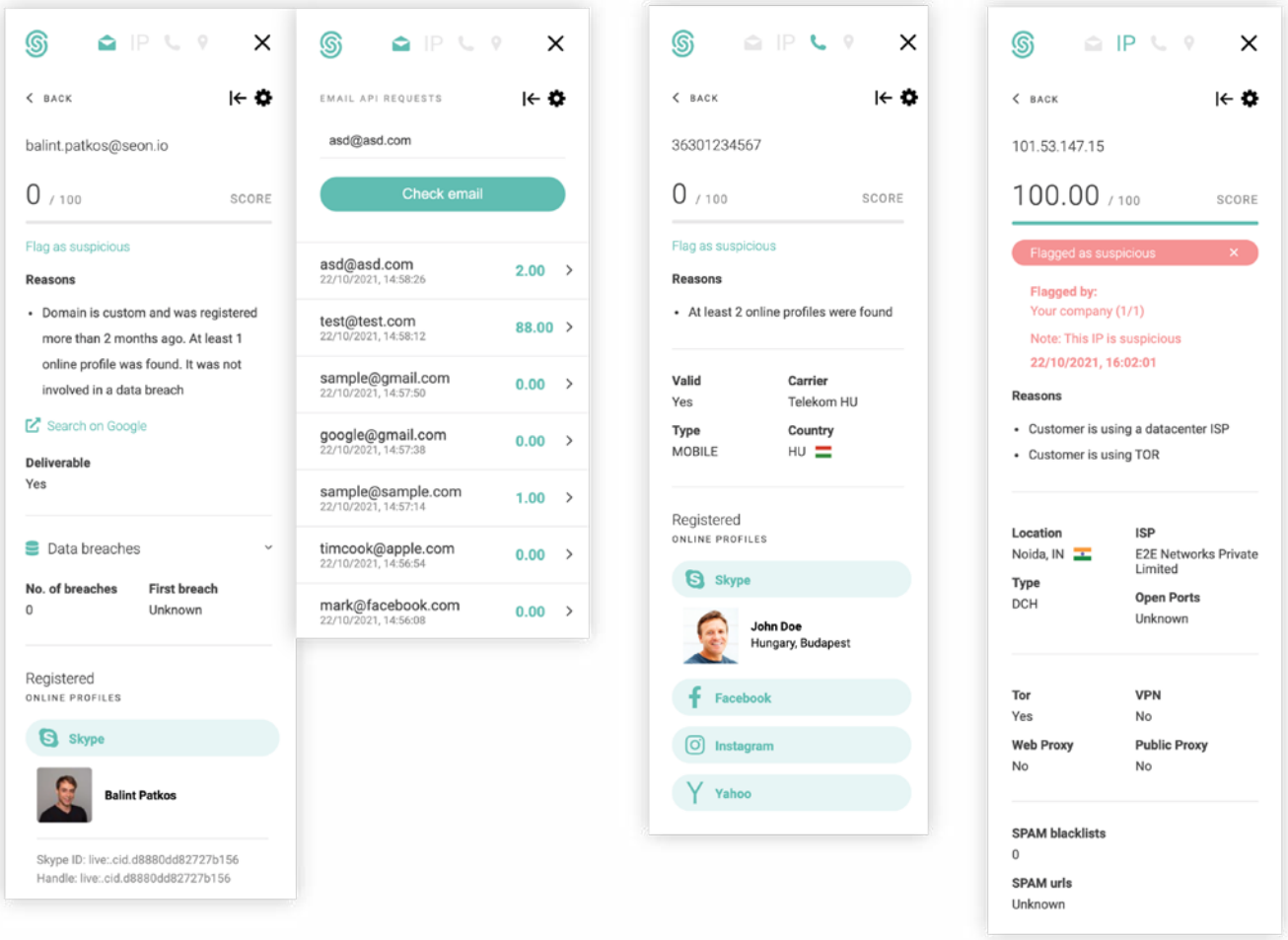
2. Verificación

En algunos casos, querrás aprender más acerca de los usuarios sin pedirles ninguna verificación. Esto es absolutamente posible gracias al proceso conocido como análisis de huella digital, también referido como “datos alternativos basados en KYC”.

Se empieza por recoger puntos de datos sobre los usuarios en cuanto aterrizan en su sitio web. Esto puede basarse en una dirección IP o en el tipo de dispositivo que utilizaron para conectarse a él, gracias a la huella digital del dispositivo. Para realizar este análisis, solo necesitarás información básica como:

- **una dirección IP**
- **una dirección de correo electrónico**
- **un número de teléfono**

La opción del número de teléfono es especialmente interesante, ya que la 2FA se está convirtiendo cada vez más en la norma. Esto empuja a los defraudadores a utilizar números de teléfono falsos o números virtuales, que pueden ser detectados por su plataforma de prevención del fraude.



Con las herramientas de enriquecimiento de datos correctas, puedes extraer suficiente información para identificar inmediatamente alertas respecto a usuarios maliciosos. Por ejemplo, podrías encontrar como sospechoso lo siguiente:

- **usuarios sin presencia en redes sociales;**
- **usuarios utilizando VPNs, proxys sospechosas o TOR;**
- **aquellos en dispositivos no categorizados;**
- **aquellos cuyas IPs aparecen en listas negras de spam.**

Todos estos datos ayudan a crear una puntuación de riesgo, lo cual te dará una idea de qué tan probable es que esa persona sea o no real. Puedes utilizar esta puntuación

para aprobar o declinar automáticamente el proceso de incorporación **con mucha más confianza.**

¿Cómo?

Información de dispositivo: no solo algunos dispositivos son más riesgosos que otros, sino que se pueden detectar a criminales recurrentes mediante las conexiones del dispositivo. De manera similar, la información del dispositivo puede revelar anomalías tales como zonas horarias conflictivas o configuraciones de idioma comparadas con quien el usuario dice ser.

Información de IP: cuando se trata del fraude, proxies, VPNs y Tor son fundamentales. Detectarlos pronto, puedes bloquear fácilmente intentos maliciosos, y filtrar intentos repetidos o automáticos.

Información de correo electrónico: al llevar a cabo una búsqueda inversa de correo electrónico en redes sociales y cotejar la base de datos Have I Been Pwned de correos electrónicos filtrados, puedes evaluar rápidamente si el usuario es una persona existente o no.

Información telefónica: aunque no se recomienda confiar en los SMS para la autenticación de dos factores, un número de teléfono puede utilizarse en la puntuación de riesgo. Puedes utilizar las búsquedas CNAM/HLR para determinar si se trata de un operador virtual o, mejor aún, averiguar el nombre registrado de ese número.

Contraseña: los hashtags de las contraseñas pueden arrojar conexiones sorprendentes de los usuarios, ya sea una frase común en un idioma determinado o la frase de contraseña favorita de un defraudador. También puedes utilizar los hashtags de las contraseñas para proteger a tus usuarios de la apropiación de cuentas, cotejándolos con contraseñas filtradas conocidas y obligando a los usuarios a elegir una alternativa más segura.

Información de la dirección: la dirección puede compararse con la dirección IP del usuario para determinar si la distancia entre ambas es factible o no.

Información de la tarjeta: es cada vez más común pedirle al usuario los detalles de pago por adelantado, en lugar de al momento de comprar, ya que mejora la experiencia de transacción. Puedes utilizar este paso para verificar si la tarjeta tiene o no fondos con un cargo de prueba, pero también puedes llevar a cabo una búsqueda BIN para obtener información del titular de la tarjeta.

Al disponer estos pasos uno después del otro, aplicando puntajes de riesgo en cada detalle, al momento en que el usuario termina de registrarse, sabrás exactamente con quién estás tratando y **si deberías o no permitirles acceder a tu plataforma.**

Esto crea una poderosa capa defensiva alrededor de tus servicios incluso antes de que los usuarios lleguen a una página de transacción. ¿La mejor parte? Los usuarios buenos

no notarán nada ya que todas estas verificaciones se ejecutan tras bambalinas sin agregar fricción, mientras que los defraudadores verán cómo sus intentos fallan repetidamente, frustrándolos lo suficiente para que se rindan.

3. Fricción dinámica

¿Pero qué pasa cuando la puntuación de riesgo no es conclusiva y necesitas solicitar información adicional? Este es exactamente el proceso que conocemos como fricción dinámica y, para explicarlo, ayuda a desglosar la idea del KYC en procesos ligeros y pesados.

La ventaja de usar el método de fricción dinámica es que puedes usarlo en la fase de KYC ligero para filtrar a los usuarios no deseados. Aquellos que son defraudadores obvios que utilizan identificaciones robadas no llegarán hasta la siguiente fase.

Sin embargo, si logran llegar y aún así representan un riesgo, entonces puedes solicitar una verificación KYC pesada, como lo describimos anteriormente.

¿Qué herramientas deberías utilizar para completar un perfil de usuario?

Ya sea para tus propias verificaciones KYC o para reducir las solicitudes que utilizan datos fraudulentos, necesitas enriquecer los datos de los usuarios tanto como sea posible.

En SEON, tenemos una serie de herramientas diseñadas para este propósito. Estas incluyen nuestro módulo de análisis de IP, para todo lo relacionado con el tipo de conexión; nuestra solución de huella digital del dispositivo, que observa la configuración de software y hardware (dispositivo y navegador, por ejemplo); nuestros módulos de análisis de enriquecimiento de datos de correo electrónico y teléfono, los cuales agregan datos desde bases de datos abiertas para obtener un panorama 360° de los clientes.

Las herramientas de análisis de teléfono y correo electrónico son particularmente útiles gracias a nuestra característica de búsqueda inversa, la cual recolecta información de más de 35 redes sociales incluyendo la foto de perfil de alguien, biografía, presencia en redes sociales y la última fecha en línea.

Nuestros clientes usan esos datos para estimar el riesgo de aprobación, acelerar las revisiones manuales e incluso para cobranzas.

Concluir un proceso de incorporación digital sin fricciones

Retornando a nuestro punto respecto a la fricción, ahora podemos equilibrar la seguridad y la experiencia de usuario en la incorporación. Sí, querrás escalar tu base de usuario tan fácil y rápido como sea posible, pero no querrás dejar la puerta tan abierta como para que cualquiera pueda entrar.

La respuesta, por tanto, está en unas herramientas de seguridad flexibles y adaptables para su onboarding digital. Equilibrar los procesos de KYC ligeros y pesados ayudará a reducir el fraude sin crear obstáculos para aquellos con un historial limpio.

Aunque siempre hay un elemento de prueba y error al equilibrar la seguridad y establecer un proceso de incorporación fácil. Equilibrar los procesos KYC ligero y pesado ayudarán a reducir el fraude sin crear obstáculos para aquellos con un historial limpio.

Es por ello que hemos creado una gama de herramientas que proporciona a las organizaciones un control total de los límites de riesgo durante la experiencia de incorporación, lo que incluye la detección durante la fase de verificación de identidad y la toma de decisiones asistidas con machine learning para la comprobación de identidad.

Aquí es donde se encuentra la clave de este acto de equilibrio: si agregas demasiados pasos de verificación puedes estar seguro de que nunca pagarás multas de AML o KYC. Pero si los haces demasiado exhaustivos los usuarios irán a otro lado. La clave está en desplegar un mejor proceso de cumplimiento KYC que te de control total sobre la cantidad de fricción sin sacrificar la seguridad.

Fuentes:

Kraken Security Labs: Your Fingerprint Can Be Hacked For $5. Here's How.

Have I Been Pwned (HIBP): ';–have i been pwned?

Naked Security: A photo will unlock many Android phones using facial recognition

SEON

Para ver cómo SEON puede ayudar a su empresa a prepararse para el futuro, visite seon.io

O programe ahora una llamada de presentación de productos personalizada.

Visite nuestro sitio web

Programe una llamada

SEON Technologies Ltd.
seon.io

info@seon.io
+44 20 8089 2900