What's next

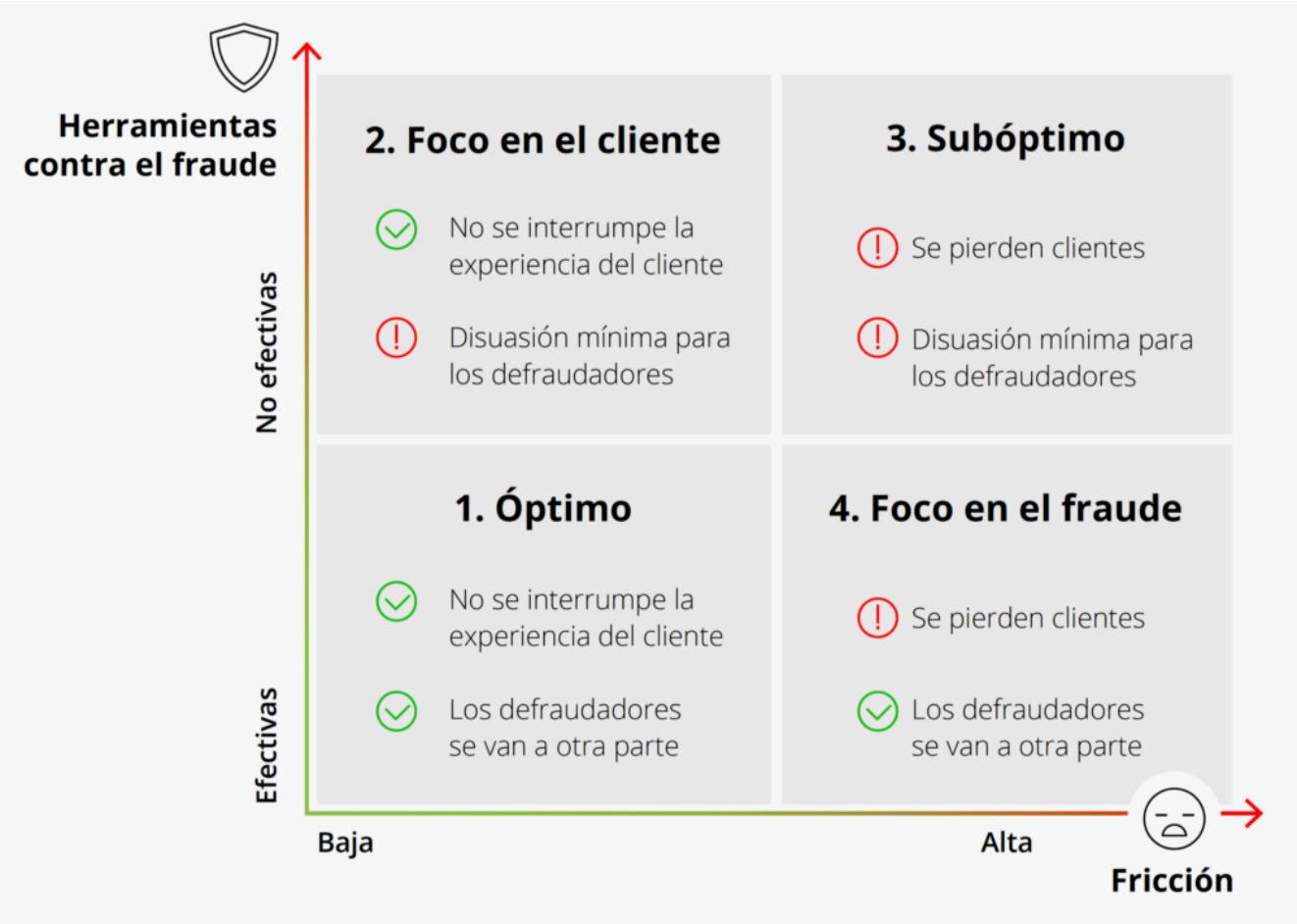
Empresa

Fraude o fricción

Nos gusta pensar que las personas son buenas por naturaleza. Sin embargo, asumir esto ciegamente en los negocios podría suponer importantes pérdidas financieras. Los estafadores podrían aprovecharse. La biometría se ha convertido en un factor importante para determinar el riesgo en segundo plano, sin que los clientes sean conscientes de que se están haciendo comprobaciones.

Simon Marchand
Posted 24 noviembre 2020

Para equilibrar el comportamiento fraudulento con la fricción, es fundamental identificar las herramientas más adecuadas para su negocio y sus clientes. Las herramientas seleccionadas deberán ser el resultado de una combinación de criterios tales como el presupuesto disponible, las personas y el tiempo de implementación.



El objetivo de cualquier negocio consiste en acercarse todo lo posible al escenario “Óptimo” de la Figura 1. Este es un equilibrio difícil de alcanzar, especialmente porque la efectividad de los recursos asignados dependerá, en parte, de su competencia.

Si tiene competidores directos y todos están en el recuadro “Óptimo”, esto significa que cuando los defraudadores encuentren una brecha de seguridad, la explotarán (desplacémonos a “Foco en el cliente”) hasta que se implementen más herramientas para detenerlos (lo que significa un movimiento hacia “Óptimo” o “Foco en el fraude”). No obstante, si su competencia se encuentra en “Subóptimo”, entonces será menos probable que el fraude se incremente en su negocio, al menos en el corto plazo.

Este enfoque simplificado muestra que una evaluación continua de su posición en el mercado y de la calidad de sus herramientas es clave para alcanzar sus objetivos de crecimiento minimizando las pérdidas financieras no deseadas provocadas por el fraude.

Mantener unos índices de fricción bajos es un excelente punto de partida para valorar qué herramientas conviene implementar. Históricamente, esto significaba buscar un equilibrio en

la cantidad de información que se recopilaba del usuario para determinar si era un cliente legítimo o no. Con la evolución de la biometría la situación ha cambiado. Ahora es posible recopilar información muy valiosa de los clientes con un esfuerzo mínimo por su parte. **Y lo que es mejor: para un defraudador es mucho más difícil hacer mal uso de estos datos o replicarlos.**

El empleo de la biometría puede regularse para ajustarlo al nivel de riesgo más apropiado. Por ejemplo, los datos sobre el comportamiento, incluyendo los patrones del habla, pueden ser recopilados en segundo plano con el consentimiento del cliente, sin que tenga que cambiar su comportamiento habitual de compra, y sin que se le pida que realice pasos adicionales durante este proceso. La mayoría de los clientes podría avanzar en la compra y/o contratación de servicios basándonos sólo en este análisis. Para aquellos que sean identificados como clientes de mayor riesgo, podrían utilizarse herramientas adicionales como pedirles un selfie o que aporten una contraseña de voz. La biometría es lo suficientemente flexible como para emplearla en muchos puntos a lo largo del recorrido del cliente desde que accede a su cuenta hasta que finaliza la compra. La recopilación pasiva de datos posibilita una experiencia mucho más fluida y con menor fricción. Cabe recordar que los clientes también valoran que su seguridad se tome en serio, y a menudo están dispuestos a realizar algunas acciones sencillas para garantizarla. Esto puede tener un impacto positivo sobre la percepción de su marca. De una u otra forma, la biometría constituye una barrera muy poderosa frente a los defraudadores, que tienen que esforzarse más para alcanzar sus objetivos, y esto seguramente les animará a abandonar e irse a otra parte.

Tags: autenticación, biometría, experiencia de usuario, fraude, fricción, seguridad

More Information

Descargar

Opus Research selecciona a Nuance como el mejor proveedor de biometría frente a 19 competidores, en el Intelligent Authentication and Fraud Prevention Intelliview Report. Consigue el reporte ahora mismo.

Download

About Simon Marchand

En la actualidad, Simon desempeña la función de Chief Fraud Prevention Officer para la división de seguridad y biometría en Nuance Communications. Simon es miembro Certificado de la Asociación de Examinadores de Fraude y posee una amplia experiencia en prevención de fraude, detección, seguridad y autenticación en los sectores banca y telecomunicaciones. Antes de Nuance, Marchand ocupó puestos de responsabilidad en los departamentos de prevención de fraude de compañías como Laurentian Bank y Bell, con sede en Montreal, y más recientemente en la Orden de Administradores Colegiados de Québec, donde dirigió su programa de inspección profesional. Marchand trabaja en estrecha colaboración con los clientes de Nuance para diseñar estrategias de autenticación y prevención de fraude basadas en tecnología biométrica que ayudan a detener a los criminales al tiempo que reducen el esfuerzo y la fricción de los clientes. Comparte regularmente su experiencia en diversas conferencias y asociaciones de todo el mundo y habla sobre los riesgos del fraude y el uso ético de la biometría en los medios.

View all posts by Simon Marchand