NUANCE | WHAT'S NEXT BLOG

Autenticación y Prevención del Fraude, Interacción con el cliente multicanal

"A mí no me pasará" – ¿Por qué la autenticación es tan importante para el cliente?

Brett Beranek | Vice President & General Manager, Security & Biometrics

25 febrero 2021

No es fácil alcanzar el equilibrio entre lograr que los clientes se sientan seguros y cómodos al realizar transacciones con su banco e introducir fricción en su experiencia online. En los últimos años los consumidores han desarrollado una mayor conciencia acerca de los riesgos que entrañan estas operaciones debido a los robos de datos, los ataques de phising y las estafas de las que habitualmente se hacen eco los medios de comunicación. Sin embargo, son muchos los consumidores que no relacionan las noticias que leen con las operaciones que realizan online. Por lo tanto, para cualquier entidad financiera es un activo de gran valor conseguir que el cliente sea en todo momento consciente de los procesos que garantizan su seguridad sin que ello le genere molestias adicionales. Aprovechar la biometría es una forma de lograrlo.

Como si el pasado año no nos hubiese deparado ya suficientes desafíos, el 31 de diciembre de 2020 fue la fecha límite para la implementación de la normativa PSD2 y la autenticación reforzada del cliente (SCA) en Europa. Esta regulación de los pagos digitales tiene un impacto en los consumidores cada vez que acceden a su información financiera en una sucursal bancaria o en la banca online, o cuando realizan compras de bienes y servicios online, aunque no está claro que la industria esté completamente preparada.

Lo que sí está claro es que esto ha supuesto grandes cambios para muchos consumidores y que la educación del consumidor sobre la normativa de autenticación reforzada SCA ha sido inconsistente. En el mejor de los casos, cuando los consumidores han accedido a sus cuentas, se les ha notificado que se avecinan cambios y se les ha preguntado si su información básica de contacto, como el correo electrónico y el número de teléfono, está actualizada. Sin embargo, **a medida que algunos bancos han comenzado a introducir estos cambios, los clientes se han visto sorprendidos y, en ocasiones, se han sentido frustrados al comprobar que no pueden realizar algunas tareas con tanta facilidad como antes.**

Como en tantas otras cosas, hasta que no son víctimas de brechas de seguridad y violaciones de sus datos, las personas se sienten "a salvo" pensando que estos problemas no les afectarán directamente. Ahora bien, cuando se ven afectadas, reaccionan instintivamente compensando en exceso, minimizando la información que comparten y agregando mayores niveles de autenticación a sus cuentas.

Sea cual sea la situación en que se encuentre un consumidor, lo cierto es que en Europa y desde finales de 2020, los clientes han tenido que acostumbrarse a que se les soliciten pasos adicionales de verificación, debido a la implementación de la normativa de autenticación reforzada SCA. Lo que significa que cuanto más sencillo sea el proceso, más exitosa será la interacción.

La biometría, como el reconocimiento facial, voz o huellas dactilares, es la opción ideal para cumplir con la normativa y proporcionar seguridad sin perder en ningún momento la experiencia del cliente. El hecho de que una encuesta reciente realizada por Mercator[1] haya revelado que en la actualidad el 41% de los propietarios de teléfonos inteligentes usan datos biométricos para autenticarse en sus terminales, y que se prevé que este porcentaje aumente hasta el 66% en 2024, demuestra que las personas están cada vez más dispuestas a confiar en la biometría, y que su uso sólo podrá incrementarse a medida que la autenticación se produzca en el servidor, además de en el dispositivo. Un hecho que permite aprovechar esta funcionalidad en múltiples canales y dispositivos, ya sea el teléfono móvil, el ordenador, la TV o un dispositivo IdC (Internet de las Cosas) específico.

Tener una visión completa del cliente es fundamental para la industria bancaria. Dado que la biometría puede implementarse a través de cualquier canal, ya sea en una sucursal bancaria, por teléfono, en un dispositivo móvil u online, proporcionando una experiencia fluida y sin interrupciones, será posible aplicar medidas de seguridad a nivel de cliente, en lugar de hacerlo por interacción o dispositivo. La capacidad de recopilar datos biométricos de forma centralizada no sólo permitirá a los bancos tener una visión completa del cliente y de las interacciones con sus cuentas, sino que también podrán gestionar datos mucho más ricos y útiles con los que tomar decisiones más precisas. De este modo protegerán a sus clientes del riesgo de fraude minimizando la fricción durante su experiencia.

La simplicidad de la biometría, al no ser necesario recordar contraseñas ni respuestas a preguntas clave, o llevar otros dispositivos encima, sumada al hecho de que se requieran dos cosas y que una de ellas sea un elemento físico inherente a cada individuo, proporciona al consumidor la sensación de que su seguridad es un asunto que se toma en serio, a la vez que resulta más difícil falsear o replicar sus datos. Además, en el caso de los procesos gestionados centralmente, el proceso es más fácil si cabe, ya que un análisis más profundo permite aplicar una seguridad más precisa y el usuario puede ser reconocido en múltiples dispositivos, incluso en aquéllos que no son de su propiedad como, por ejemplo, cuando acude a una sucursal.

Encontrar una manera de autenticar a los consumidores minimizando las molestias, así como la probabilidad de verse obligados a reiniciar el proceso si una variable de autenticación cambia, se convertirá en un factor diferenciador para aquellos negocios que necesitan autenticar a los clientes, como las entidades financieras y los emisores de tarjetas. Esto se ve confirmado por los cambios que evidencian los comportamientos tanto de los consumidores como de los defraudadores. Las soluciones multicanales pueden proporcionar una experiencia fluida y perfectamente ajustada a estos cambios.

Hoy en día, las entidades financieras informan de un aumento del 250% en las transacciones digitales. Y McKinsey estima que en la "nueva normalidad" de la COVID-19, el porcentaje de necesidades bancarias básicas gestionadas en la sucursal podría caer hasta un 5%. En este mundo nuevo y al igual que siempre, **los bancos necesitan asegurarse de estar interactuando con el verdadero cliente, pero ello supone un reto mucho mayor teniendo en cuenta la naturaleza remota de la interacción.**

Las condiciones de crisis crean nuevos riesgos para las entidades financieras a medida que aumenta el fraude. **Una entidad financiera con la que trabajamos experimentó un aumento del 400% en los intentos de fraude durante la irrupción de la pandemia. Para los muchos canales digitales que aún dependen de los métodos de autenticación antiguos (PIN's y contraseñas), y particularmente en las organizaciones más consolidadas, este aumento puede resultar muy perjudicial.** La forma de autenticar a los clientes en los canales digitales se ha estancado, especialmente si la comparamos con la que emplean los *contact centers*. Aquí no hay opciones de autenticación con dispositivo, sino que la autenticación debe resolverse a través de un servidor, lo que abre la puerta para que la biometría reemplace por completo a la autenticación basada en el conocimiento. Nuevamente, esto permite que el cliente recorra fácilmente el proceso de autenticación con una interrupción mínima de su experiencia, pero también transmite la idea de que la seguridad es una parte fundamental de su interacción. En consecuencia, **la experiencia del *contact center* debe extenderse a los canales digitales, priorizando la seguridad de los datos y la precisión en la autenticación.**

La capacidad biométrica es clave para satisfacer las necesidades de seguridad, al tiempo que fomenta el compromiso del cliente, máxime cuando el universo de lo digital sigue creciendo. En el caso de los bancos, servirá para que los clientes disfruten de una mejor experiencia con la certeza de que su información está a salvo y sus operaciones son seguras.

Tags: Autenticación Biométrica, Experiencia de cliente, Prevención de fraude

More Information

Ver ahora

Dos grandes empresas del panorama español con grandes proyectos con la voz como protagonista. No te pierdas esta mesa redonda con Enrique Tellado, CEO de EVO Banco y Pedro Serrahima, director de Desarrollo de Negocio Multimarca en Telefónica para conocer su experiencia y el impacto en el negocio desde el lanzamiento de EVO VoiceID y Telefónica Age Detection.

Learn more

About Brett Beranek

Brett Beranek es General Manager de la división de biometría y seguridad en Nuance Communications. Antes de unirse a Nuance, ha trabajado durante más de una década como responsable de desarrollo de negocio y marketing en distintas empresas de software y seguridad. Brett posee una amplia experiencia en el campo de las tecnologías biométricas, donde es importante destacar su papel como socio fundador de la startup Viion Systems, empresa de desarrollo de software de reconocimiento facial. Su conocimiento en materia de seguridad abarca una amplia variedad de tecnologías que incluyen, desde la biometría de huella dactilar, hasta tecnologías de análisis de videos para el entorno de la seguridad física y reconocimiento de matrículas. Brett es licenciado en comercio, con la especialidad de sistemas de información por la Universidad McGill y posee un máster en marketing por la Sloan School of Management de Massachusetts Institute of Technology.

View all posts by Brett Beranek