El fraude en el *contact center* y canales digitales.

Estrategias para encontrar el equilibrio entre prevención y experiencia de cliente.

NUANCE

Índice

Contact centers: el talón de Aquiles de la prevención del fraude

El fraude está aumentando en todos los canales de interacción con el cliente, bien se trate de servicios financieros, agencias gubernamentales, telecomunicaciones o compañías aéreas. Pero los expertos están de acuerdo: el *contact center* es quizás el canal más vulnerable y el objetivo más fácil para los ladrones.

Los *contact centers* se han convertido en los **«epicentros de vulnerabilidad en muchas organizaciones».**[1]

Gartner

Un análisis más profundo
Imagine que es el director de un *contact center* de una empresa de servicios financieros. Uno de sus agentes responde a una llamada entrante de Pablo García, quien dice tener problemas para acceder a su cuenta corriente porque ha olvidado la contraseña. Su agente sigue el protocolo, le pregunta a Pablo cuál es su número de cuenta y número de la seguridad social, y le pide que responda a unas preguntas de autenticación. Satisfecho con las respuestas, el agente activa el protocolo de restablecimiento de contraseña y el cliente puede acceder a la cuenta. **Pero, ¿debería?**

Cuando suena el teléfono en el *contact center*, surge una pregunta crucial: el que está al otro lado del teléfono, ¿es un cliente o un estafador que trata de robar dinero, productos o servicios? ¿es el verdadero titular de la cuenta o alguien empleando técnicas de ingeniería social y de violación de datos preparado para vaciar una cuenta? Este tipo de preguntas son cada vez más importantes. Mientras que las empresas de telecomunicaciones, servicios financieros y las agencias gubernamentales han tomado innumerables medidas para reforzar la seguridad de sus recursos *online*, los delincuentes han comenzado a fijarse en un objetivo mucho más atractivo y lucrativo: ***el contact center***.

Es lo que Gartner llama «un epicentro de vulnerabilidad», donde muchas organizaciones tienen problemas para limitar la extensión del impacto. Sin duda, el desastre financiero para la organización es devastador, independientemente del sector. Las instituciones gastan una cantidad de dinero considerable para luchar contra los estafadores responsables de las pérdidas de miles de millones de dólares que suponen los robos, el tiempo perdido o los gastos generales añadidos. Para el cliente (pensemos en un Pablo García real), el fraude en el *contact center* puede vaciar algo más que una cuenta. Puede acabar con la confianza del cliente. Y en el mercado en general, si la reputación de la organización se ve afectada, el público puede perder la confianza que tenía depositada en ella, incluso para siempre.

Esto se debe a que las redes de fraude organizadas están analizando las instituciones financieras y otras organizaciones con el fin de encontrar la información que necesitan para acceder a los fondos de los clientes y a la información de sus cuentas. El *contact center*, cuyo personal tiene la función de prestar un servicio amable y de alta calidad, es a menudo el punto que ofrece menos resistencia, lo que se traduce en una «elección fácil» para los estafadores. Esta creciente marea de fraude supone altos riesgos financieros y empresariales que no son aceptables y que las empresas responsables deben abordar inmediatamente.

En este libro blanco se analizan los retos a los que se enfrentan las organizaciones y cómo la biometría de voz, multimodo y de comportamiento, puede detectar y evitar el fraude con éxito a la vez que mejora la experiencia del cliente por ejemplo, gracias a un esfuerzo menor en los procesos de autenticación y verificación.

1 Phillips, Tricia and Care, Jonathan. (2 de marzo de 2017). Don't Let the Contact Center Be Your 'Achines Heel' of Fraud Prevention. Gartner.

La identificación y verificación tradicionales ya no son eficaces

La incidencia del fraude en el *contact center* continúa creciendo con rapidez. Gartner calcula que, para el año 2020, el 75% de las organizaciones que se relacionan con sus clientes por varios canales sufrirán un ataque de fraude y el *contact center* será el punto de entrada principal. La mayoría de los servicios de voz de los *contact center*s están aislados, orgacionalmente y arquitectónicamente, de otros canales, como el autoservicio web o las aplicaciones móviles, lo que significa que no están protegidos por las cuidadosas medidas de prevención del fraude y prevención de pérdidas orientadas a los canales digitales.[2]

Quizás esto es así porque estos *contact centers* son a menudo el eslabón más débil. Como observó la empresa Aite Group dedicada a la investigación de mercado: **«El fraude que se apropia de cuentas llega tantas veces a través del contact center que este debería llamarse el 'canal de facilitación del fraude multicanal'».**[3]

El alcance de estos ataques también es importante. Según un estudio de 2018 de Javelin Strategy & Research[4]:

– El número de víctimas de fraudes por suplantación de identidad aumentó un 8%, hasta llegar a los 16,7 millones de consumidores en EE. UU.
– Los estafadores obtuvieron 1,3 millones más de víctimas en 2017, robando 16 800 millones de dólares a los consumidores.
– La apropiación de cuentas se triplicó el año pasado, lo que supuso 5100 millones de dólares en pérdidas.
– Las víctimas pagaron una media de 290 dólares de sus bolsillos y dedicaron 15 horas de su tiempo para solucionar estos incidentes.

Por desgracia, la identificación y verificación tradicionales están ya lejos de poder controlar un acceso no autorizado. Como indica Forrester, una contraseña de ocho caracteres de una palabra que no esté en el diccionario, con dos números distintos, una letra mayúscula y dos caracteres especiales puede adivinarse... en nueve horas. Dado el aumento de ordenadores en clúster y la capacidad de computación que crece de manera exponencial, dentro de poco las contraseñas ya no protegerán las transacciones de alto riesgo o en las que haya que hacer pagos.[5]

¿Otra razón por la que la seguridad basada en contraseñas morirá? Las brechas de seguridad. Los consumidores han soportado un bombardeo constante de violaciones de datos, y sus datos personales y credenciales de usuario se han visto comprometidos en numerosas ocasiones: 145 millones de cuentas de Equifax, 130 millones de cuentas de Heartland Payment Systems, 110 millones de cuentas en Target, 250 millones de cuentas de Epsilon, y 15 millones de cuentas en Experian, entre muchas otras. Como resultado de estas y otras muchas brechas de seguridad, el paradigma tradicional de PIN y contraseña ha llegado a su fin. Además de que los estafadores pueden eludirlo fácilmente, los clientes odian tener que recordar, y cambiar, las distintas contraseñas complejas que necesitan para tantos sitios web y servicios. Según la analista Avivah Litan de Gartner, entre el 15-30% de los clientes de una empresa no superan la prueba de identificación, mientras que el 60% de los delincuentes sí lo hace.

75%

Para el año 2020, el 75% de las organizaciones que se relacionen con sus clientes por varios canales sufrirán un ataque fraudulento en el que el *contact center* será el punto de entrada principal.[2]

2 Phillips, Tricia and Care, Jonathan. (2 de marzo de 2017). Don't Let the Contact Center Be Your 'Achines Heel' of Fraud Prevention. Gartner.
3 Inscoe, Shirley. (miércoles, 27 de abril de 2016). Contact Centers: The Fraud Enablement Channel. Aite Group. Retrieved from: https://www.aitegroup.com/report/contact-centers-fraud-enablement-channel
4 Pascual, Al; Marchini, Kyle; y Miller, Sara. (6 de febrero de 2018). 2018 Identity Fraud: Fraud Enters a New Era of Complexity. Javelin Strategy & Research. Obtenido de: https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity#
5 Csar, Andras y Spiliotes, Alexander. (6 de febrero de 2018). Forrester Research TechRadar: Biometric Authentication, Q1 2017 "Adoption of User- and Mobile-Friendly Biometrics will Kill the Password." Forrester Research.

Según Javelin Strategy & Research, el 95% de las llamadas que entran al *contact center* son de clientes de verdad.[6] Pero esto significa que el 5% restante presenta dificultades de validación, porque el *contact center* tiene cuatro vulnerabilidades clave:

– **Fácil acceso a los datos del consumidor**
Casi cualquier elemento de la identidad de una persona puede comprarse o comerciarse, incluidos los números de la seguridad social, datos de las tarjetas de crédito, credenciales para la banca *online*, y mucho más.

– **Anonimato**
Gracias a las violaciones de seguridad que hacen que grandes bases de datos personales identificables estén disponibles, es fácil para los delincuentes anónimos de lugares remotos mezclar y fabricar datos para crear identidades sintéticas.

– **Velocidad**
Las herramientas digitales permiten a los delincuentes perpetrar el fraude mucho más rápido que en el mundo físico. Por ejemplo, los 'bots' pueden crear exponencialmente más aplicaciones de fraude.

– **Debilidad en los controles complementarios**
Las soluciones que antes eran eficaces están fracasando y se están quedando atrás. Por ejemplo, depender demasiado de la identificación del dispositivo es una debilidad de control que está siendo atacada.

Simplemente, ahora es mucho más fácil que un «Pablo García» falso responda a las preguntas del agente del *contact center*, se apropie de una cuenta y la vacíe, bien sea robando puntos de fidelización de una compañía aérea, ayudas del gobierno, artículos caros, o fondos de pensiones. Sin embargo, añadir más dificultad al proceso de verificación tampoco es una opción atractiva.

La biometría al rescate

Está claro que para fortalecer esas vulnerabilidades hay que invertir en procesos que no gustan demasiado y hay que aumentar los controles, sobre todo si las empresas y organizaciones adoptan la transformación digital. «Aquí existe una discrepancia: los consumidores están contentos porque su banco los protege, pero se frustran porque la protección les dificulta abrir cuentas y hacer compras», señaló T J Horan en FICO. «Cuando se trata de transformación digital, una experiencia de cliente fluida va a ser fundamental. Las empresas que puedan equilibrar esto y la necesidad de detener el fraude serán las que salgan ganando».[7]

Para lograr el equilibrio entre la experiencia del cliente y la necesidad de seguridad, los expertos de la industria están usando cada vez más la biometría de voz como estrategia importante para verificar la identidad en numerosas aplicaciones de seguridad. Gartner, por ejemplo, recomienda a los *contact centers* implementar tecnología de prevención del fraude para mejorar la autenticación del cliente y reducir la duración de las llamadas de los clientes legítimos, identificando al mismo tiempo llamadas de alto riesgo para analizarlas en profundidad. Para esto, es fundamental integrar la biometría de voz con el fin de detectar con rapidez las llamadas fraudulentas y la transición entre cuentas, y para identificar huellas de voz fraudulentas confirmadas.[8]

A medida que los usuarios exigen una identificación sencilla en cualquier canal, **las soluciones de biometría van consiguiendo una atención significativa para la autenticación y, especialmente, para la prevención**... Además, a medida que **se vayan adoptando, más rápido desaparecerá el método que menos gusta a los usuarios: las contraseñas.**

Forrester Research, "TechRadar™: Biometric Authentication, 1.er trimestre de 2017

6 Pascual, Al; Marchini, Kyle; y Miller, Sara. (6 de febrero de 2018). 2018 Identity Fraud: Fraud Enters a New Era of Complexity. Javelin Strategy & Research. Obtenido de: https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity#

7 Orem, Tina. (11 de julio de 2018). Everybody Is Sick & Tired of Online Security Measures, Poll Finds. Credit Union Times. Obtenido de: https://www.cutimes.com/2018/07/11/everybody-is-sick-tired-of-online-security-measure/

8 Phillips, Tricia and Care, Jonathan. (jueves, 2 de marzo de 2017). Don't Let the Contact Center Be Your 'Achines Heel' of Fraud Prevention. Gartner.

Afortunadamente, la biometría puede desempeñar una función clave en el *contact center* y en múltiples canales de comunicación a través de la autenticación y la prevención del fraude. Comienza por la voz. Cuando el supuesto titular de la cuenta llama al *contact center*, un sistema biométrico compara su voz con la «huella de voz» guardada con el fin de confirmar que la persona que llama es quien dice ser. No hace falta proporcionar más información ni responder a preguntas de verificación, así que el proceso es rápido y seguro. Esto permite al agente de ventas continuar con confianza y ofrecer una experiencia totalmente personalizada al cliente.

Como se ha dicho antes, se encuentra una coincidencia de voz entre las huellas de voz guardadas para aproximadamente el 95% de todas las personas que llaman. El 5% restante debe someterse a unos niveles de análisis adicionales. En la mayoría de los casos, no son estafadores Aunque no son los titulares de las cuentas, tienen permiso de estos para realizar una transacción en su nombre. Podría tratarse de un cónyuge, una secretaria, un cuidador, o un contable. Pero, desafortunadamente, en un gran número de casos, la persona que llama es una persona no autorizada que trata de estafar al titular de la cuenta y a la institución.

Caso práctico de biometría

Pensiones BBVA Bancomer solicita la biometría de voz de Nuance para verificar fes de vida

Con clientes en todo México, Pensiones BBVA Bancomer necesitaba una forma rápida, precisa y rentable de verificar la fe de vida de las personas mayores y otros pensionistas, un proceso que se lleva a cabo dos veces al año. El banco utilizó Nuance Security Suite para la autenticación y detección del fraude en su sistema de respuesta de voz interactiva (IVR), *contact center*, móviles y canales web. Por medio de la biometría de voz, el sistema analiza la voz única de más de 70 000 clientes que se han registrado en el sistema.

Los resultados:

– Reducción significativa del tiempo necesario para verificar la fe de vida.
– Prestación de servicio a un mayor número de pensionistas.
– Servicio eficiente y atento a los pensionistas.
– Procesos administrativos simplificados y automatizados con menor coste.

«Las tecnologías que son transparentes para el usuario final, como la analítica conductual y las tecnologías de huella de voz, son las preferidas por las instituciones financieras (IF), que reservan la intrusión y el coste de una autenticación de mayor nivel solo para un pequeño porcentaje de clientes... Cuando se les preguntó si pensaban invertir en tecnología de voz como método para proteger sus *contact centers*, **el 25% de las IF indicó que ya cuenta con un programa piloto o está trabajando en una implementación en producción, mientras que otro 40% tiene pensado adoptar tecnología de voz en los próximos 1-2 años».**

Aite Group[9]

9 Inscoe, Shirley. (27 de abril de 2016). Contact Centers: The Fraud Enablement Channel. Aite Group. Obtenido de: https://www.aitegroup.com/report/contact-centers-fraud-enablement-channel

Más allá de la autenticación y la voz

Mientras que algunos proveedores hacen hincapié en la autenticación, otros se centran en la prevención del fraude. Combatir el fraude exige una estrategia de doble flanco de autenticación y prevención del fraude para mejorar la experiencia del cliente y reducir el esfuerzo de los clientes legítimos mientras se impide un acceso fraudulento.

Y como los estafadores no se limitan a un solo canal de interacción y cada vez se dirigen más al *contact center* (el consabido talón de Aquiles del fraude), las empresas deben implementar medidas de **identificación de clientes y prevención del fraude** que lleguen a todos los canales de interacción (por ej., autoservicio web, aplicaciones móviles, y el *contact center*).

Asimismo, estas medidas omnicanal deben hacer uso de las modalidades biométricas y no biométricas. Cuando la persona que llama no pasa la prueba de comprobación de huella de voz, el *contact center* no puede simplemente negarse a prestarla servicio, ya que esto generaría cientos de miles de clientes enfadados con razón. En lugar de ello, el *contact center* puede llevar a cabo una serie de comprobaciones biométricas y no biométricas para continuar, con cuidado, de una forma que reduzca o elimine la exposición al fraude.

– **Comparación con una lista de estafadores conocidos**
Cuando la voz del titular de la cuenta no coincide con la huella de voz guardada, el *contact center* puede comparar la grabación con las voces de una lista de estafadores conocidos (personas que han llevado a cabo con anterioridad transacciones fraudulentas). Si se encuentra una coincidencia, la llamada entra en una «zona gris» y se gestiona de forma diferente. El *contact center* podría llamar al titular de la cuenta para confirmar el acceso y las transacciones. Podría bloquear la cuenta y las transacciones y enviar un correo al titular de la cuenta. Sin embargo, simplemente hacer preguntas de seguridad es, cada vez menos, un método eficaz de selección.

– **Análisis de la conversación**
Si la voz de la persona que llama no coincide con la huella de voz del titular de la cuenta, pero tampoco es la huella de voz de un estafador conocido, podemos utilizar tecnología biométrica patentada para analizarla, para conocer el patrón de habla, la estructura de las frases e incluso la gramática, lo que se conoce como «ConversationPrint™» (huella de conversación). En lugar de fijarse solo en las características de la voz, esta prueba compara la forma de hablar de la persona que llama con las características del habla conocidas del titular de la cuenta para comprobar si coinciden. Además, al igual que con las huellas de voz, podemos comparar huellas de conversación con las de una biblioteca de estafadores conocidos y decir con confianza:
- Esta no es la forma de hablar normal del titular de la cuenta.
- Esta es la forma de hablar de un estafador anterior.
Igualmente importante desde un punto de vista omnicanal, la tecnología de reconocimiento del patrón del habla ConversationPrint no se restringe a las llamadas de voz. También puede aplicarse a *chats* de texto con los agentes, una forma muy habitual entre los estafadores de intentar hacerse pasar por el titular de la cuenta, ya que pueden disimular el género y los acentos al hablar. El análisis de la conversación integrado es una forma sencilla, fácil y personalizada de permitir a un agente identificar al consumidor de forma transparente para prevenir el fraude, todo ello sobre la marcha.

Combatir el fraude exige una estrategia de doble flanco de autenticación y prevención del fraude para mejorar la experiencia del cliente y reducir el esfuerzo de los clientes legítimos mientras se impide un acceso fraudulento.

– **La biometría de comportamiento**
Los clientes de comportan de manera diferente y la biometría puede reconocer y evaluar dichos comportamientos para compararlos con patrones conocidos, tanto para titulares de cuenta como para estafadores. Estos patrones puede ser la forma de teclear (fuerza al pulsar la tecla, desplazamiento y secuencia), uso del ratón, e incluso cómo sujeta o usa el *smartphone* el usuario (incluida la presión, área de pulsación y mucho más). La biometría de comportamiento, por supuesto, puede mejorar la prevención del fraude en distintos canales de interacción.

Caso práctico de biometría

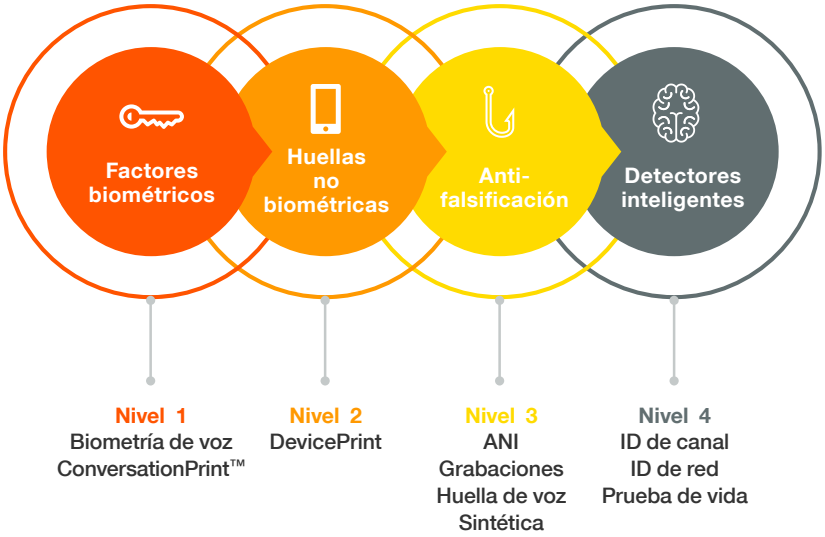
Barclaycard reduce el fraude de apropiación de cuentas un 40%
Los premios 'Card and Payment Awards' reconocen la excelencia e innovación en las industrias de pagos y tarjetas del Reino Unido e Irlanda. En 2015, el cliente Barclaycard consiguió el premio en la categoría 'Mejor Seguridad o Desarrollo Antifraude'.

Al explicar por qué se eligió a Barclaycard, el jurado escribió: «Barclaycard quería proteger a sus clientes sin procedimientos complejos. Barclaycard implementó una solución dinámica para detectar el fraude que usaba la biometría de voz de Nuance para proteger a sus clientes sin procesos disruptivos. El responsable de los servicios financieros recopiló una exhaustiva biblioteca de voces de estafadores conocidos y, por medio de la tecnología de Nuance, implementó un sistema piloto casi en tiempo real que comparaba las voces entrantes con las de la lista negra. Al audio entrante se le asigna una puntuación de riesgo y las alertas las analizan un grupo de expertos agentes de fraude de Barclaycard que, cuando es necesario, se ponen en contacto con los clientes, protegen la cuenta del cliente, y añaden nuevos estafadores a la lista negra.

Como primera institución financiera del Reino Unido en implementar la biometría de voz, Barclaycard **redujo el fraude de apropiación de cuentas en más del 40% en un breve periodo y confirmó que casi el 75% de las alertas de alto riesgo eran fraudes.** Los efectos adversos en los clientes fueron inapreciables. Asimismo, el contacto puntual y transparente con las víctimas de fraudes ha generado experiencias de cliente muy positivas».
Card and Payment Awards Ltd., Londres

Niveles de seguridad

Aunque la biometría puede ofrecer niveles de autenticación y prevención del fraude con excepcional precisión, existen otros indicios que podemos observar automáticamente y que pueden ser posibles delitos. De manera conjunta, las técnicas biométricas y no biométricas crean varias capas de seguridad.



Por medio de estos «niveles de seguridad», podemos buscar otros indicios cuando una huella de conversación o de voz no coinciden con las del titular de la cuenta:

– **ID del dispositivo**
Una empresa puede registrar el ID del dispositivo único de un ordenador portátil o teléfono móvil. Si este ID no coincide con el que está registrado, el sistema puede emitir una alerta. Por supuesto, se presentan dos dificultades. En primer lugar, los usuarios cambian y actualizan sus dispositivos, creando problemas en las transacciones que menoscaban la experiencia del cliente. Otro factor quizás más problemático es que algunas interacciones las llevan a cabo familiares, cuidadores y otras personas de confianza, que pueden acceder fácilmente a los dispositivos registrados del titular de la cuenta.

– **Medidas antifalsificación**
Algunas de las técnicas no biométricas clave para prevenir el fraude incluyen la validación del número de la llamada (ANI), detección de grabaciones, no coincidencias de género, y detección de voces sintéticas.

– **Detectores inteligentes**
Si el dispositivo del titular de la cuenta se asocia a los EE. UU., pero la llamada que llega al *contact center* se origina en un país remoto, o el *chat* entrante llega de una dirección IP conocida por ser un punto problemático (o incluso un número de teléfono que es fraudulento), podría tratarse de un intento de fraude. Incluso algo tan sencillo como un canal de voz puede servir de advertencia. Si el titular de la cuenta llama normalmente desde un teléfono fijo, pero la llamada entrante llega de un teléfono móvil desechable, podría tratarse de un fraude.

Alto perfil, alta prioridad, alto impacto

Con una plataforma robusta para la identificación y la prevención del fraude, las agencias gubernamentales, empresas de servicios financieros y otras compañías pueden obtener ventajas significativas.

– **Menores costes**
  Las soluciones integradas para la identificación y prevención del fraude pueden mejorar considerablemente el rendimiento del *contact center*: desde un mayor uso de las opciones de autoservicio, a reducciones en la duración media de una llamada y en el tiempo de gestión de llamadas de alto riesgo. Todo esto mejora directamente el balance final.
– **Experiencia del cliente mejorada**
  Las iniciativas de prevención del fraude implementadas correctamente deben reducir (o casi eliminar) cualquier problema disruptivo en el *contact center*. Esta mejora transparente en la seguridad y experiencia del cliente se traduce en un mayor grado de satisfacción de los clientes (fidelidad del cliente). Los clientes prefieren la biometría de voz por su simplicidad, transparencia y efectividad.
– **Mayor satisfacción del agente**
  Al eliminar la necesidad de interrogar (y, potencialmente, irritar) al cliente, los agentes del *contact center* ven cómo la biometría de voz simplifica su trabajo y mejora su satisfacción, lo que puede reducir el absentismo y la rotación laboral. Los agentes pasan más tiempo ayudando a los clientes y menos tiempo tratando asuntos de seguridad.
– **Diferenciación de marca**
  Para las instituciones financieras, la biometría está creando un importante punto de diferenciación que están promoviendo enérgicamente. Los consumidores reconocen la importancia de la seguridad, y las instituciones financieras publicitan cada vez más el uso de la biometría directamente a los clientes.
– **Reducción del fraude**
  Obviamente, la métrica más importante es la cantidad de dinero que pueden ahorrarse las instituciones al prevenir o mitigar el fraude. Un cliente de Nuance indicó que había evitado pérdidas por un valor de 6 millones de USD en las primeras seis semanas tras la implementación.

Caso práctico de biometría

Banco multinacional
Nuance encargó a Forrester Consulting un estudio sobre el impacto económico, TEI (Total Economic Impact™) y el ROI de Nuance Security Suite. Para comprender mejor las ventajas, costes y riesgos, Forrester entrevistó a un banco multinacional que llevaba años utilizando Nuance Security Suite para identificar de forma segura a las personas que llamaban a los *contact centers* y monitorizar las llamadas procedentes de intentos de fraude.

Antes de Nuance, el banco utilizaba los procesos estándar de la industria para identificar a los clientes junto a sistemas internos para monitorizar el fraude. Cuando los clientes llamaban para pedir asistencia, muchos de ellos no recordaban las contraseñas bancarias ni las respuestas a las preguntas de seguridad, por lo que los agentes debían verificar su identidad a través de diversas preguntas. Esta frustrante experiencia aumentó la duración de las llamadas y los costes operacionales. Mientras tanto, las pérdidas vinculadas al fraude en el *call center* continuaron aumentando.

Después de su implementación en el Reino Unido, el banco tiene pensado adoptar la biometría de voz a nivel global durante los próximos años. Según las entrevistas y los análisis de datos agregados, Forrester concluyó que Nuance Security Suite tenía el impacto financiero a tres años siguiente:

24 314 327 de USD en beneficios en comparación con 8 350 049 en costes... **Resultado: valor neto actual de 15 964 278 USD,** y... Un **ROI del 191%**.

24.3
millones de USD

Un banco multinacional consiguió beneficios de 24,3 millones de USD tras la implementación de la biometría de voz, frente a los 8,3 millones de USD en costes, lo que deriva en un valor neto actual de 15,9 millones de USD.

191%

En el mismo banco multinacional, se obtuvo un ROI del 191% tras la implementación de la biometría de voz.

Conclusión

Ahora más que nunca, la identificación y la prevención del fraude son la base de las estrategias proactivas para la interacción con clientes de casi cualquier organización que se relacione con ellos, incluidas las empresas de servicios financieros, agencias gubernamentales, y comercios de artículos de gran valor. También está cada vez más claro que las organizaciones ya no pueden considerar sus canales silos independientes. Las comunicaciones omnicanal requieren iniciativas y estrategias de seguridad omnicanal.

Asimismo, estas estrategias –que comprenden la identificación y la prevención del fraude– deben unir defensas por capas biométricas y no biométricas para crear una experiencia del cliente satisfactoria, sin fraude y sin problemas en los canales de voz y canales digitales.

A medida que las contraseñas y la autenticación mediante respuestas a preguntas van desapareciendo, la biometría y otras estrategias de prevención del fraude que abarcan otros canales de comunicación (por ej., autoservicio web y aplicaciones móviles) son cada vez más importantes.

Próximos pasos: descubra más cosas sobre Nuance Security Suite
Nuance ayuda a las empresas de distintas industrias a prevenir el fraude y reducir al mismo tiempo el esfuerzo y los problemas de legitimar a los clientes. Descubra cómo puede conseguir resultados similares:

– Conozca Nuance Security Suite
– Envíe un correo electrónico a pilar.blasco@nuance.com para solicitar una llamada de 15 minutos con un especialista en prevención del fraude.

Acerca de Nuance Communications, Inc.
Nuance Enterprise está reinventando la relación entre las empresas y los consumidores a través de soluciones para los clientes que hacen uso de la inteligencia artificial. Nuestro objetivo es ser el proveedor líder del mercado de soluciones inteligentes de autoservicio y servicio asistido para grandes empresas de todo el mundo. Estas soluciones están diferenciadas por tecnologías cognitivas, del habla, biometría de voz, asistente virtual y chat web, y permiten una prestación de servicio al cliente multicanal en IVR, móvil, web, y llamadas entrantes y salientes, todo ello potenciado con el diseño y desarrollo de un equipo de servicios profesionales global. Prestamos servicio a empresas Fortune 2500 de todo el mundo con modelos de venta directa y a través de distribuidores.

NUANCE

NUAN–CS–3591–01–WP-SPA, 21 de agosto de 2018