OneSpan
Be bold. Be secure.

APERTURA DIGITAL DE CUENTA

CÓMO TRANSFORMAR Y PROTEGER EL PROCESO DE APERTURA DIGITAL DE CUENTA

WHITE PAPER

RESUMEN EJECUTIVO

Los clientes esperan un proceso de apertura de cuenta totalmente digital, disponible online y en sus móviles. Los bancos, instituciones crediticias y otras instituciones financieras necesitan ofrecer experiencias de apertura y contratación de cuenta a través de dispositivos móviles y centradas en el cliente, para atraer clientes y promover el crecimiento.

La verificación de la identidad digital supone un desafío

El proceso de apertura de cuenta tiene el potencial de repercutir en la lealtad de los clientes a largo plazo, así como en la rentabilidad, retención, y participación de los gastos del cliente. A pesar de esto, la verificación de identidad digital sigue siendo uno de los procesos que más desafíos presentan para la digitalización de la instituciones financieras. Si bien las instituciones financieras tradicionales están avanzando en este ámbito, sigue existiendo un alto índice de abandono durante la solicitud, un aumento en los niveles de fraudes de identidad, y cada vez más competencia de nuevos bancos, que ha hecho que sea urgente modernizarse.

Tecnologías y tendencias para transformar la apertura de cuenta y la verificación de la identidad

En base a extensas entrevistas y consultas con nuestra base de clientes y analistas de Gartner y Aite Group, este informe resalta las tecnologías, tendencias y consideraciones clave a la hora de digitalizar y proteger la experiencia de apertura de cuenta.

Los propietarios de negocios y directivos senior en experiencia digital, transformación digital y prevención de fraudes se beneficiarán de estas recomendaciones respecto a cómo transformar esta área estratégica del negocio. Al suplementar los sistemas principales con funcionalidades tales como verificación de la identidad digital, automatización de las contrataciones, firma electrónica y analíticas de riesgo basadas en el aprendizaje automático, las instituciones financieras pueden superar los desafíos a los que se están enfrentado a la hora de digitalizar la apertura de cuenta.

ÍNDICE DE CONTENIDOS

INTRODUCCIÓN

> Una buena experiencia del cliente está estrechamente correlacionada con la inclinación de dicho cliente a realizar otra adquisición, y crea lealtad a la marca. Cada experiencia de autenticación online deficiente aumenta el riesgo de atrición de los clientes y pérdida de ventas. Crear una experiencia del cliente omni-canal, consistente y memorable, debe ser una obsesión para su compañía."
>
> **Forrester**
> **The Identity And Access Management Playbook, 2018**

Los nuevos clientes esperan poder abrir una cuenta online. Como resultado de ello, los bancos y otras instituciones financieras necesitan ofrecer la apertura digital de cuenta a través de los canales online y móvil. A pesar de la demanda por parte de los clientes de un servicio de apertura de cuenta completamente digital, muchos bancos no ofrecen experiencias de apertura de cuenta totalmente digitales, y en algunos de los aspectos del proceso de captación, tales como la verificación de identidad, se requiere que los solicitantes acudan a la sucursal. El/La posible cliente comienza el proceso de apertura de cuenta online, pero a continuación debe firmar contratos impresos o presentar documentos de identidad en persona. Estos procesos manuales ralentizan el proceso de apertura de cuenta y frustran a los solicitantes, lo que a menudo hace que abandonen el proceso de apertura de cuenta.

Las experiencia negativa del cliente lleva a altos índices de abandono

La imposibilidad de ofrecer un proceso de apertura de cuenta totalmente digital significa que bancos, instituciones crediticias y otras instituciones financieras están perdiendo clientes frente a competidores y nuevos bancos que ofrecen a los usuarios la posibilidad de abrir cuenta de forma totalmente a distancia o remota. Según la Analista Senior Tiffani Montez, de Aite Group, "las tasas de abandono siguen estando entre un 65% y un 95%, dependiendo del producto."1 Si la experiencia de los clientes es deficiente, es posible que los solicitantes acudan a proveedores de servicios financieros que les permitan finalizar el proceso de apertura de cuenta en una sola sesión.

Verificar la identidad de un(a) solicitante a distancia de forma digital, a la vez que se protege el proceso de apertura de cuenta contra fraudes, ha supuesto un desafío para las instituciones financieras. Avances en los métodos de verificación de la identidad digital, tales como verificación de documentos de identidad y comparación facial, están cambiando esto.

Las experiencias totalmente digitales promueven el crecimiento

La necesidad no satisfecha de una experiencia de apertura de cuenta totalmente digital presenta una tremenda oportunidad de crecimiento. Para ofrecer experiencias de apertura de cuenta excepcionales, a la vez que se protege a usuarios e instituciones financieras de fraudes, las instituciones financieras deben priorizar tecnologías que:

- ✓ Digitalicen las partes clave del proceso de apertura de cuenta, tales como los métodos de verificación de identidad digital y las firmas electrónicas.
- ✓ Ofrecen una plataforma que se integre con soluciones existentes y de terceras partes
- ✓ Aprovechen al máximo el flujo de trabajo
- ✓ Detecten y mitiguen el fraude en tiempo real

La experiencia y la seguridad de los usuarios están intrínsicamente relacionadas, y los mejores procesos de apertura de cuenta a distancia ofrecerán la conveniencia que los clientes demandan, a la vez que ofrecen las medidas de seguridad y de lucha contra el fraude en las que confían las instituciones financieras.

> Las instituciones financieras deberían reemplazar los procesos manuales de autenticación de clientes en sucursal, centro de atención telefónica, y equipo de operaciones por reconocimiento facial, en lugar de hacer preguntas basadas en conocimiento.[3]
>
> **Tiffani Montez**
> **Analista Senior de Banca Minorista, Aite Group**

TENDENCIAS CLAVE EN VERIFICACIÓN DE IDENTIDAD DIGITAL

La verificación de identidad digital es un paso clave en el proceso de apertura de cuenta a distancia, ya que cumple con los requisitos de Conozca a Su Cliente (KYC por sus siglas en inglés) que las instituciones financieras deben cumplir a la hora de captar nuevos clientes. KYC es un paso importante en la lucha contra el fraude. Al verificar la identidad de los solicitantes, las instituciones financieras pueden hacer comprobaciones para asegurar que el/la solicitante no es un(a) criminal o impostor(a).

En una encuesta realizada en 2018 por Aite Group sobre procesos de apertura de cuenta en grandes instituciones financieras, el 63% de los encuestados indicaron que era probable que implementaran captura de datos móvil y verificación de documentos de identidad para cuenta corrientes, de ahorros y tarjetas de crédito en 1-2 años.[2]

El sector de servicios financieros invierte cada año ingentes cantidades de dinero para atraer y captar nuevos clientes. Desgraciadamente, gran parte de esto se pierde cuando el/la solicitante se da de bruces contra un obstáculo durante el proceso de apertura de cuenta. Este punto de fricción es a menudo el paso inicial de verificación de identidad, en el que la institución financiera debe realizar comprobaciones KYC para asegurar que el/la solicitante es quien dice ser y que no está intentando cometer un fraude.

Hoy en día, los enfoques de verificación de identidad en el sector de servicios financieros se clasifican en dos categorías:

1. **Verificación manual en persona:** Los/Las solicitantes online y móviles se ven forzados a ir a la sucursal para verificar su identidad y firmar los documentos. Esto introduce un alto nivel de fricción e impide a los/las solicitantes que finalicen el proceso en una única sesión.
2. **Métodos de verificación online no fiables y de alta fricción:** Un método de verificación de identidad digital utilizando comúnmente es la Autenticación basada en conocimiento (KBA por sus siglas en inglés). La KBA consiste en que el/la solicitante responda a una serie de preguntas que se verifican usando indagaciones en oficinas de crédito y bases de datos de terceras partes. Desgraciadamente, la KBA se considera un proceso de alta fricción, que requiere que los/las solicitantes recuerden y respondan a preguntas de carácter personal basadas en datos públicos. Además, la KBA se ha vuelto menos fiable debido a las filtraciones de datos a gran escala que se han producido en los últimos años. Los métodos de verificación manuales en persona resultan inaceptables para consumidores que demandan una experiencia de apertura de cuenta digital sencilla, conveniente y sin fricciones.

Los métodos de verificación de identidad actuales son:

ALTA FRICCIÓN	DEMASIADO LARGOS	NO SEGUROS
El 65-95% de los/las usuarios/as abandonan el proceso de apertura de cuenta debido a pasos de alta fricción tales como el requisito de tener que ir a la sucursal o responder a preguntas basadas en conocimientos.[4]	Las verificaciones de identidad en persona impiden que los/las solicitantes puedan finalizar el proceso de apertura de cuenta en una única sesión. Cuando el proceso de apertura de cuenta se alarga debido a la verificación obligatoria en persona de la identidad, aumentan los índices de abandono.	La autenticación basada en conocimiento, que se basa en “algo que usted sabe”, siempre han implicado una alta fricción, pero antiguamente prevenían fraudes. Las múltiples filtraciones de información a gran escala hoy en día han hecho que los modelos que sólo se basan en preguntas basadas en conocimiento sean menos eficaces.

TENDENCIA 1: LOS USUARIOS ESTÁN DISPUESTOS A REALIZAR ACCIONES QUE ESTABLECEN CONFIANZA

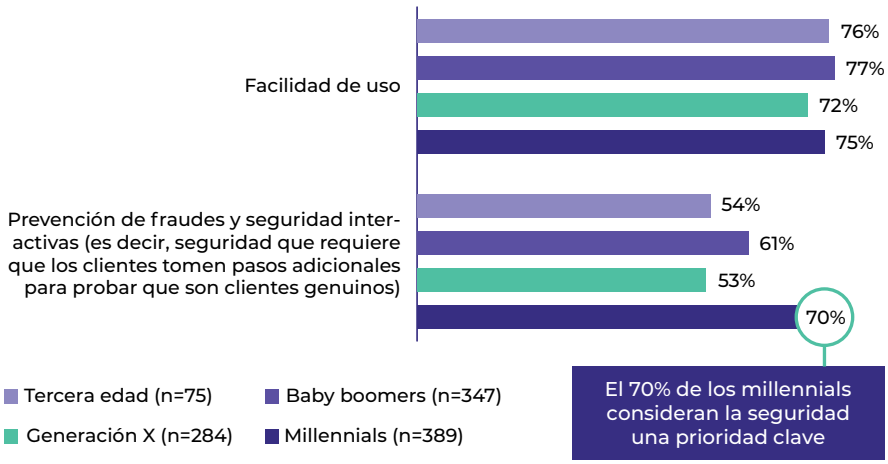
La facilidad de uso es muy importante para los/las usuarios/as a la hora de abrir una cuenta a distancia, pero también lo es la seguridad. Los/as solicitantes quieren asegurarse de que sus datos están seguros y que sus cuenta no pueden ser manipuladas. Por lo tanto, los/las solicitantes están dispuestos/as a aceptar algunos pasos relacionados con la seguridad durante el proceso de apertura de cuenta. Estas acciones para mejorar la confianza forjan una relación más sólida entre el/la usuario/a y el banco.

En una encuesta a consumidores realizada por Aite Group, se encontró que el 70% de los millennials consideraban la seguridad como una prioridad clave a la hora de realizar transacciones con instituciones financieras online.[5]

Esto sugeriría que existe una clara diferencia entre fricción "buena" (fricción que protege al usuario y establece confianza) y fricción "mala" (fricción que frustra y trastorna la facilidad de uso). Los consumidores de hoy en día, especialmente las generaciones futuras, son más conscientes de la necesidad de contar con acciones que mejoren la confianza, protejan su cuenta y ayuden a impedir fraudes.

El punto en el que se introduce la fricción en el recorrido de los clientes es a menudo igual de importante que el modo en el que se introduce. Gartner se refiere a este proceso de establecimiento de confianza como "intimidad progresiva". Al comienzo de la relación entre un(a) cliente y una institución financiera, ésta aún no se ha ganado la confianza del/la cliente. No obstante, una vez que se establece la confianza, el/la usuario/a aceptará más fricción para mantener su cuenta segura.

Prioridades de los consumidores respecto a funcionalidades de banca online



Fuente: Aite Group.

TENDENCIA 2: LA VERIFICACIÓN DE IDENTIDAD DIGITAL DE MÚLTIPLES CAPAS OFRECE UNA EXPERIENCIA DE USUARIOS ÓPTIMA Y PROTEGE CONTRA EL FRAUDE

La apertura digital de cuenta presenta un doble desafío: Las instituciones financieras deben cumplir con sus objetivos de riesgo y conformidad, a la vez que aseguran una experiencia de usuario sin fisuras.

La verificación de identidad digital de múltiples capas a través de una única plataforma permite a las instituciones financieras acceder a un amplio abanico de servicios de identidad y verificación ofrecidos por terceras partes. De este modo, las instituciones financieras pueden seleccionar los mejores tipos de verificación para su caso de uso y canal, mejorar la experiencia de usuarios y reducir riesgos.

Un enfoque basado en plataforma ofrece unos índices de éxito más altos y posibilita la conmutación por error en el caso de un fallo en la verificación o la no disponibilidad del proveedor. Esto a su vez elimina la necesidad de una intervención manual y reduce la tasa de abandono de clientes. Todo ello permite a las instituciones financieras ofrecer una experiencia óptima a los clientes y protegerse del fraude en el proceso de solicitación, por no hablar del fraude de apropiación fraudulenta de cuenta, que supone el mayor desafío para las instituciones financieras.[6]

Las ventajas de un enfoque de identidad digital de múltiples capas son:

1. **Ampliable:** La posibilidad de seleccionar los mejores tipos de verificación para optimizar las tasas de adopción y acceder a nuevas formas de verificación según éstas van saliendo al mercado.
2. **Flexible:** La posibilidad de acceder a diferentes proveedores de verificación a través de una única plataforma.
3. **Auditable y ejecutable:** La posibilidad de capturar un registro auditable completo del proceso de verificación de la identidad.
4. **Configurable:** Las instituciones financieras pueden seleccionar múltiples tipos de verificación y crear un flujo de trabajo de tipos de verificación basados en un conjunto de reglas o flujo de trabajo de identidad (p.ej., riesgo o geografía).

El enfoque de múltiples capas permite a las instituciones financieras obtener una perspectiva de 360° de los/las solicitantes

> La captura y verificación automática de documentos de identidad son relativamente nuevas en el mercado y están ganando tracción en numerosos sectores económicos. [...] En general, el 90% de las instituciones financieras indican que planean implementarlas en los dos próximos años.[7]
>
> **Aite Group**

LOS MEJORES MÉTODOS DE VERIFICACIÓN DE IDENTIDAD DIGITAL

VERIFICACIÓN DE DOCUMENTOS DE IDENTIDAD

La verificación de documentos es un método de verificación de identidad digital utilizado para comprobar si el documento de identidad del/la solicitante (p.ej. pasaporte, carnet de identidad, carnet de conducir, etc.) es legítimo.

Por medio de la cámara integrada del móvil o de un dispositivo portátil, la tecnología captura una imagen del documento de identidad del/la solicitante. A continuación se utilizan avanzados algoritmos de inteligencia artificial y autenticidad para analizar la imagen y calcular una puntuación de autenticidad que determina si el documento de identidad es fraudulento o genuino.

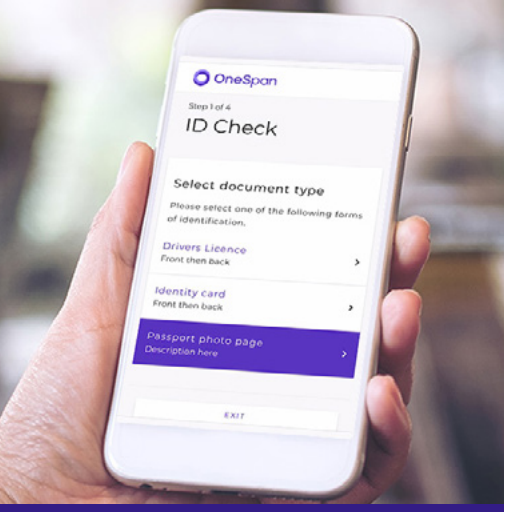
Entre los autenticadores avanzados se encuentran:

1. **Características de seguridad visibles:** Se pueden detectar características de seguridad integradas, tales como marcas de agua u hologramas, y se puede analizar su posición y aspecto.
2. **Uso y consistencia de las fuentes:** Se analizan las fuentes y se comparan con fuentes estándar para una plantilla de documento específica. Se examina el espaciado, forma y consistencia de las letras para analizar su autenticidad.
3. **Detección de esquinas redondeadas:** Se pueden verificar las esquinas redondeadas para asegurar que están de acuerdo con las plantillas.

Una vez que se ha completado la comprobación de autenticidad, la tecnología de verificación de documentos de identidad extrae datos tales como el nombre y la fecha de nacimiento del documento de identidad autentificado. Estos datos reducen la necesidad de introducir los datos manualmente y pueden compararse con datos previamente capturados (tales como datos proporcionados durante un proceso de aplicación) para probar que el/la titular del documento de identidad es la persona que está solicitando la apertura de cuenta.

La verificación de documentos de identidad permite autentificar los documentos de identidad de clientes de forma digital y en tiempo real, tanto si los usuarios se encuentran en la sucursal o a distancia. Para el consumidor, la experiencia resulta rápida y sencilla. Para las instituciones financieras, la verificación automática de documentos de identidad agiliza el proceso de apertura de cuenta, suprime un paso manual, elimina la necesidad de capacitar al personal para verificar documentos de identidad y asegura que los procesos de verificación de identidad sean consistentes y conformes, a la vez que se protege de fraudes.

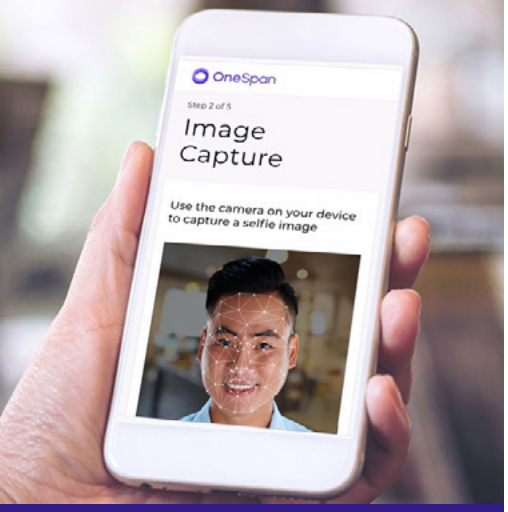
> Capturar los datos de un documento de identidad permite a una institución financiera utilizar dichos datos para rellenar automáticamente otro documento, como por ejemplo una solicitud de tarjeta de crédito o cuenta de depósito a la vista. Esto resulta mucho más sencillo para el cliente que tener que escribir todos estos datos usando un pequeño teclado de móvil, y también elimina muchos errores tipográficos que por lo general conllevan una mayor carga de labores administrativas, con lo que se mejora la eficiencia operacional. [...] Asimismo, se puede cumplir con los requisitos CSC, lo que mejora la conformidad."[8]
>
> **Aite Group**



Cómo funciona la verificación de documentos

Ventajas de la verificación de documentos de identidad:

- ✓ Contribuye a cumplir con los requisitos de lucha contra el lavado de activos y de KYC.
- ✓ Utiliza características de comparación facial para cerciorarse de que la persona que presenta el documento de identidad coincide con la persona que aparece en dicho documento.
- ✓ Un proceso completamente digital brinda una experiencia excelente al usuario. Cualquiera persona puede utilizar y acceder a la captura de imágenes por medio del móvil.
- ✓ La extracción de datos directamente del documento elimina la entrada de datos manual.
- ✓ Los documentos se pueden verificar en cuestión de segundos (de <5 minutos a <10 segundos, dependiendo del proveedor)



COMPARACIÓN FACIAL

La posibilidad de probar que un(a) usuario/a es genuino/a y está físicamente presente durante la apertura de cuenta a distancia constituye un componente clave en la lucha contra fraudes en el proceso de solicitud de apertura de cuenta. En 2017, tan sólo en Estados Unidos hubo 16,7 millones de víctimas de robo de identidad, todo un récord.[9] Con los altos niveles de robo de identidad, resulta esencial que las instituciones financieras verifiquen que un(a) usuario/a es genuino/a durante el proceso de apertura de cuenta.

Debido a las filtraciones de información y vulnerabilidades de seguridad de los SMS, los métodos tradicionales de verificación de identidad, tales como KBA y autenticación de dos factores por SMS, no resultan ya fiables para verificar a los usuarios durante la apertura de cuenta a distancia. Esto está haciendo que las instituciones financieras recurran a la verificación de documentos de identidad y la comparación facial para verificar a posibles clientes de forma segura.

La comparación facial se utiliza del siguiente modo para probar que un(a) solicitante está presente durante la transacción:

1. **Verificación de documento:** Se utiliza la verificación de documento para verificar la autenticidad del pasaporte, carnet de identidad o carnet de conducir del/la solicitante.
2. **Selfie:** Una vez que se ha confirmado la autenticidad del documento de identidad, se le pide al/la solicitante que se haga un selfie con su dispositivo portátil.
3. **Comparación biométrica:** La tecnología de comparación facial compara la imagen del selfie con la imagen del documento de identidad verificado, para probar que la persona verificada está presente durante el proceso de apertura de cuenta.

Las tecnologías de comparación facial utilizan avanzados algoritmos para extraer datos biométricos de los rasgos de una persona, destilando una imagen en un conjunto de datos estandarizados. Por ejemplo, puede utilizarse la posición y tamaño de los ojos de una persona en relación entre sí como un punto de datos extraído de una imagen. Comparar dos conjuntos de datos puede determinar si dos imágenes pertenecen a la misma persona.

Si una imagen proviene de una fuente verificada anteriormente (p.ej., un pasaporte o carnet de identidad verificado por medio de verificación de documentos) y la segunda imagen es una imagen en tiempo real tomada por el/la solicitante en el momento de realizar la solicitud, se puede utilizar la comparación facial para probar su presencia.

Consideraciones de la tecnología de comparación facial

Detección de movimiento: Antes de usar una imagen capturada o selfie para el reconocimiento facial, se puede aplicar detección de movimiento a la imagen para probar que hay una presencia humana genuina y que no se ha utilizado una imagen estática de la persona de forma fraudulenta. La detección de movimiento ayuda a probar que no se ha creado una imagen de forma fraudulenta usando métodos tales como impresiones de alta resolución o vídeos grabados anteriormente.

Imagen de fuente verificada: Debe haber disponible una imagen del/la cliente con la cual hacer la comparación. Para solucionar esto, se puede utilizar la comparación facial con una funcionalidad de verificación de documento que pueda extraer una imagen fuente de un documento de identidad válido.

> La conversión digital representa la oportunidad de implementar firmas electrónicas para préstamos, lo que elimina la necesidad de firmar en una sucursal o ante notario/a, y proporciona métodos sencillos para el cliente de transferir fondos a una cuenta corriente que no implican que tenga que ir a la sucursal para realizar su primer depósito.
>
> **Aite Group**
> **Transformación de la experiencia de apertura de cuenta y captación digitales**

EL PAPEL DE LAS FIRMAS ELECTRÓNICAS

Una vez que se ha verificado la identidad de un(a) nuevo/a solicitante y se han cumplido los requisitos KYC, el siguiente desafío para mantener el proceso de apertura de cuenta totalmente digital es obtener la firma del/la cliente. Dependiendo del tipo de cuenta y las leyes y regulaciones aplicables, es posible que se requiera una firma para convenir en los términos de la cuenta, aceptar recibir documentos por vía electrónica, o acuse de recibo para las notificaciones digitales.

Para instituciones financieras y otras organizaciones que están implementando firmas y registros electrónicos, a menudo surgen preguntas en cuanto a los requisitos e implicaciones de las firmas electrónicas. Actualmente, más de 90 países han aprobado leyes que habilitan las firmas y registros electrónicos.

En Europa existen tres tipos de firma electrónica: Básica, Avanzada y Cualificada. Mientras que los dos primeros no requieren validación de identidad por parte de terceros en forma de certificado digital, el último requiere que una Autoridad de Certificación (AC) proporcione un certificado digital personal a la parte firmante, y en ciertos países es obligatorio utilizar la AC local. Por lo tanto, para posibilitar la conformidad con los requisitos legales y regulatorios de cualquier jurisdicción, es importante que una solución brinde flexibilidad para implementar cualquiera de estos tipos de firma electrónica como parte de un proceso online o móvil.

Implementar firmas electrónicas como “hacer clic para firmar” asegura la experiencia de usuario más sencilla para casos de uso a distancia. Según un informe realizado en 2018 por Celent para comparar las experiencias de apertura de cuenta móvil de los principales bancos, “dentro del contexto móvil, marcar una casilla para aceptar los términos y proporcionar una firma era todo lo que se necesitaba.” [10]

Las firmas electrónicas pueden realizarse en cualquier dispositivo (p.ej., a través de una app para móvil, o un navegador web o móvil) y pueden integrarse completamente para lograr un traspaso automatizado entre sistemas finales. Los datos digitales capturados por medio del proceso de apertura de cuenta pueden fluir a sistemas principales y utilizarse para desencadenar automáticamente procesos subsiguientes.

Las instituciones financieras reportan que los flujos de trabajo de apertura de cuenta sin papel mejoran de forma exponencial la primera experiencia con el/la cliente, eliminando la necesidad de esperar mientras se imprimen documentos o corrigen errores. Y si se hace a distancia, existe la ventaja añadida de permitir al/la cliente elegir cuándo y dónde realizan la transacción con el banco.

Para desarrollar la estrategia omni-canal de una institución financiera, las instituciones financieras pueden utilizar firmas electrónicas en múltiples canales. Para el/la cliente, imagine contar con la posibilidad de iniciar el proceso de apertura de cuenta online, pausarlo, guardar su progreso, y continuar más adelante en otro canal, como por ejemplo el móvil, sin tener que volver a introducir información ya proporcionada. Para la institución financiera, mantener un proceso omni-canal consistente contribuye a evitar las demoras, costes y errores que surgen cuando se utilizan procesos con papel y manuales.

BMO Bank of Montreal implementó la firma electrónica para simplificar y agilizar los procesos de apertura de cuenta y captación a distancia. Hoy en día, los/las nuevos/as solicitantes y los/las clientes existentes pueden abrir una nueva cuenta desde su teléfono en menos de ocho minutos. [11]

BMO Bank of Montreal

EL COSTE DEL FRAUDE

- 13.000 millones de filtraciones de información desde 201318
- Un 2,41% de los ingresos de las instituciones financieras perdido a causa del fraude[19]
- 5.100 millones de dólares estadounidenses en pérdidas por fraude de identidad en 2018[20]
- Se calcula que las instituciones bancarias estadounidenses gastarán 599 millones de dólares estadounidenses para combatir el fraude en solicitudes en 2020[21]

CONSIDERACIONES DE SEGURIDAD Y CONFORMIDAD

Los ciberataques a bancos e instituciones financieras están aumentando en volumen, complejidad y velocidad. Según Forbes, los ciberataques tienen como objetivo a las empresas de servicios financieros 300 veces más a menudo que las de otros sectores.[12] Los atacantes se dirigen a instituciones financieras para acceder a datos confidenciales de clientes que pueden usar para cometer acciones fraudulentas.

Además de causar ansiedad a las víctimas, el fraude cuesta a las instituciones financieras y sus compañías de seguros cantidades de dinero significativas. LexisNexis calcula que en 2018, el coste del fraude para las compañías de servicios medianas y grandes que operan a nivel internacional supuso el 2,41% de sus ingresos.[13]

Teniendo en cuenta la escala y repercusión del fraude, resulta vital que las instituciones financieras puedan detectarlo durante el proceso de apertura de cuenta. Ya que los estafadores usan métodos cada vez más sofisticados, un sistema de prevención de fraude basado en reglas no puede por sí solo estar al día. Para ir por delante, las instituciones financieras necesitan una solución de verificación de identidad y de lucha contra el fraude basada en riesgos que aproveche la IA a través del aprendizaje automático supervisado y no supervisado.

El aprendizaje automático permite a las organizaciones analizar datos con contexto en diferentes dispositivos, aplicaciones, y transacciones, y requiere muy poco esfuerzo manual. Los algoritmos de aprendizaje automático analizan los datos de la transacción y sólo alertan de transacciones sospechosas con puntuaciones de riesgo más altas. Al detectar patrones complejos que son difíciles de identificar para humanos y para métodos más antiguos basados en reglas, este enfoque analítico basado en riesgos resulta más eficaz a la hora de detectar fraudes nuevos y emergentes.

Ataques comunes durante y después del proceso de apertura de cuenta

Durante la apertura de cuenta	Después de la apertura de cuenta
FRAUDE EN LA SOLICITUD Los estafadores usan los datos de clientes robados a través de filtraciones de información, apropiación fraudulenta de cuenta, ingeniería social, phishing o innumerables métodos diferentes, para abrir una nueva cuenta de forma fraudulenta. En 2018, las filtraciones de información expusieron 447 millones de registros a nivel internacional en los sectores de banca, empresas, educación, gobierno y salud.[15] Las filtraciones de información que exponen información personalmente identificable hacen que sea más fácil perpetrar robos de identidad y fraudes de solicitud. Además de fraudes de solicitud, el uso de identidades manipuladas, sintéticas o fabricadas va asimismo en aumento. Los estafadores alimentan las identidades sintéticas de modo que tengan registros en oficinas crediticias y números de móvil antes de usarlas para cometer fraudes. [16]	**APROPIACIÓN FRAUDULENTA DE Cuenta** Según Javelin Research, 16,7 millones de consumidores estadounidenses sufrieron un robo de identidad en 2017, más de 1 millón más que el año anterior. Mucho de esto fue causado por ataques de apropiación fraudulenta de cuenta, y las pérdidas por robos de identidad ascendieron a 5.100 millones de dólares.[17] Entre los ataques comunes que llevan a la apropiación fraudulenta de cuenta se incluyen: • **Ataques de phishing:** Los estafadores envían correos electrónicos o SMS diseñados para que el/la destinatario/a haga clic en un link que le redirecciona a un portal de banca falso o a abrir un archivo adjunto que instalará un programa malicioso que recabará credenciales. • **Ataques Troyanos y Superposiciones en banca móvil:** Los estafadores aprovechan las vulnerabilidades de los sistemas operativos para instalar programas maliciosos troyanos en el dispositivo de la víctima. Con esto superponen pantallas falsas en apps de banca legítimas para recabar credenciales bancarias. • **Programas maliciosos:** Los estafadores recaban datos a través de programas maliciosos que registran las pulsaciones del teclado o que ejecutan interposiciones, que interceptan datos a través del navegador de la víctima.

USO DE VERIFICACIÓN DE IDENTIDAD DIGITAL PARA LUCHAR CONTRA EL FRAUDE EN LAS SOLICITUDES

Las instituciones financieras por lo general han venido dependiendo de oficinas crediticias para la verificación de identidad. Uno de los problemas de este enfoque es la naturaleza estática de la información personal. Si la información personalmente identificable ha sido robada o se ha visto comprometida, los estafadores podrán usarla para abrir una nueva cuenta.

Cuando un(a) solicitante está intentando abrir una nueva cuenta, las instituciones financieras ya no pueden depender únicamente de la información estática de las oficinas crediticias para la verificación de la identidad de un(a) usuario/a. Al combinar las analíticas de riesgo con métodos de verificación de identidad digitales de múltiples capas, las instituciones financieras pueden verificar un(a) potencial cliente utilizado un enfoque sensible al contexto.

Un enfoque sensible al contexto permite tomar decisiones en tiempo real respecto a seguridad en base al riesgo total asociado con un(a) nuevo/a cliente, para manejar mejor su riesgo de fraude, especialmente en transacciones a distancia. Con una solución de verificación de identidad sensible al contexto, las instituciones financieras pueden reducir exponencialmente el fraude y generar un crecimiento superior, a la vez que brindan la mejor experiencia posible al/la usuario/a en la apertura de nuevas cuenta digitales.

ASEGURAR LA CUENTA DEL CLIENTE UNA VEZ QUE SE HA CAPTADO

Una vez que se ha captado al/la cliente y se ha abierto la cuenta, las instituciones financieras deben asegurarse de que el acceso a la cuenta del/la cliente sea seguro. Cada vez que un(a) cliente intenta acceder a la cuenta, las instituciones financieras deben autenticar la identidad del/la usuario/a para asegurar que el intento de acceso es genuino y que no ha sido iniciado por atacantes que intentan acceder a la cuenta. En una encuesta realizada por Aite Group, el 27% de los consumidores declararon que accedían a sus cuenta de banca móvil a diario, y un 47% accedían a su cuenta al menos una vez por semana.[14] Con semejante frecuencia de uso, las instituciones financieras deben autenticar a los usuarios continuamente.

Los clientes existentes deben ser autenticados por medio de una serie de métodos de autenticación digitales, como códigos de un solo uso, autenticación multifactorial, autenticación por SMS, y autenticación biométrica.

Se puede utilizar asimismo la tecnología de autenticación adaptiva para mejorar aún más la experiencia del usuario, a la vez que se proporciona el nivel de seguridad óptimo para cada transacción.

La autenticación inteligente adaptiva utiliza el aprendizaje automático para analizar el riesgo de una transacción en base a datos tales como el comportamiento del/la usuario/a, su ubicación, la integridad del dispositivo, y transacciones recientes. Al asignar puntos a estos elementos de información, esta tecnología puede aplicar una puntuación de riesgo a cada transacción y adaptar la seguridad y autenticación requerida de forma acorde a lo largo del recorrido digital del/la cliente. Esto asegura la mejor experiencia posible para el/la cliente, a la vez que protege las transacciones y los datos confidenciales de los clientes.

REGISTROS AUDITABLES DIGITALES

Para probar que se siguió un proceso de apertura de cuenta conforme, las instituciones financieras deberían capturar un registro auditable completo de lo que el/la solicitante vio e hizo exactamente durante el proceso de apertura de cuenta, incluyendo los pasos de verificación de identidad y firma.

Los registros auditables digitales prueban que la institución financiera realizó todas las comprobaciones CSC necesarias y que el/la solicitante tenía la intención de vincularse a los términos del acuerdo. Los registros auditables proporcionan un registro completo del proceso de apertura de cuenta y pueden proteger a las instituciones financieras de litigios judiciales o relacionados con la conformidad.

CÓMO ONESPAN LE PUEDE AYUDAR

En OneSpan, nuestra misión es transformar y proteger el recorrido digital de los clientes, desde su primera interacción hasta asegurar sus cuenta a lo largo de todo el ciclo de vida del cliente. Nuestras soluciones han sido diseñadas para ayudar a las instituciones financieras a brindar un experiencia de usuario diferenciada, a la vez que se protegen las transacciones financieras de los clientes y se contribuye a protegerles de fraudes. Para obtener más información, visite OneSpan.com o contacte con nosotros para hablar de sus requisitos específicos.

1 Aite Group, AI: Transforming the Digital Account-Opening and Onboarding Experience, 2018

2, 3, 4 Ibid

5 Aite Group, Digital Banking Customer Engagement: Adoption, Usage, and Satisfaction Impact Report, 2017

6, 7, 8, 18, 21 Aite Group, Application Fraud: Fighting an Uphill Battle, Diciembre 2018

9 Javelin Strategy & Research, Identity Fraud Study, 2018

10 Celent Research, The US Open: Looking at Mobile Account Opening at US Banks

11 Celent Research, BMO Digital Transformation in Personal Banking, 2017: http://bit.ly/2oUTDyW

12 Forbes, https://bit.ly/2INLaLI

13, 19 Lexis Nexis, 2018 True Cost of Fraud Study for the Financial Services Sector

14 Aite Group, AI: Transforming the Digital Account-Opening and Onboarding Experience, 2018

15 Identity Theft Resource Center, End-of-Year Data Breach Report, 2018

16 Aite Group, Synthetic Identity Fraud: The Elephant in the Room, 2018

17, 20 Javelin Strategy & Research, Identity Fraud Study, 2018

OneSpan

OneSpan permite alcanzar el éxito a instituciones financieras y otras organizaciones, al hacer avances audaces en su transformación digital. Conseguimos esto estableciendo confianza en la identidad de las personas, los dispositivos que utilizan, y las transacciones que son determinantes para sus vidas. Creemos que esta es la base de una habilitación de negocios mejorada y de crecimiento. Más de 10.000 clientes, incluyendo más de la mitad de los 100 primeros bancos globales, confían en las soluciones de OneSpan para proteger sus relaciones y procesos comerciales más importantes. Desde la integración digital a la reducción de fraudes, pasando por la gestión del flujo de trabajo, la plataforma unificada y abierta de OneSpan reduce costes, acelera adquisiciones por parte del cliente, y aumenta la satisfacción del cliente.

OBTENGA MÁS INFORMACIÓN SOBRE LA APERTURA DE CUENTA DIGITAL

CONTACTE CON NOSOTROS

info@OneSpan.com
OneSpan.com