White Paper

Fácil, Pero Potente:

Cómo las Compañías de Servicios Financieros Pueden Beneficiarse de la Seguridad Respaldada por la Biometría

AWARE

781.687.0300 | sales@aware.com | www.aware.com

Aware is a leading global provider of software products and solutions for biometric identification and authentication. They are used for variety of applications including financial services, enterprise security, border management, and law enforcement. Aware is a publicly held company (NASDAQ: AWRE) based in Burlington, Massachusetts.

Es difícil superar la ventaja de la internet. Películas desde la comodidad de sillones reclinables, eventos deportivos con un sinfín de botanas cerca en la cocina, o la selección y entrega de abarrotes sin moverse del sofá – se espera que todo esté disponible a través de dispositivos conectados. Se estima que 3.8 mil millones de personas tienen un smartphone , lo que representa casi la mitad de la población mundial.

Los bancos y las compañías de servicios financieros también han tenido que adaptarse a este nuevo escenario digital, proporcionando a sus clientes nuevas formas de acceder a sus cuentas y manejarlas. Desde el punto de vista del cliente, es difícil superar la conveniencia de depositar cheques, revisar estados de cuenta y mover dinero en cualquier momento o en cualquier lugar que elijamos. La pandemia de COVID-19 sólo intensificó una tendencia ya al alza, aumentando aún más la demanda de soluciones financieras basadas en dispositivos móviles que no requieran visitas presenciales. Se espera que el número de usuarios activos de la banca en línea en todo el mundo crezca a más de 2.5 mil millones para el 2024, superando los 2.1 mil millones hoy en día.

Esta combinación de la omnipresencia de los smartphones y el deseo de conveniencia ha contribuido a actualizar los procedimientos tradicionales de incorporación y autenticación de clientes financieros, resaltando la importancia de proporcionar a los clientes financieros un medio tanto para abrir, como para acceder a sus cuentas con seguridad desde un cualquier lugar.

Sin embargo, los que participan en servicios financieros saben que esto no es una tarea fácil. Nunca faltan las personas malintencionadas. Lo que es peor, las instituciones financieras también enfrentan una estricta supervisión reglamentaria como parte de las políticas contra el lavado de dinero, lo que significa que es sumamente importante para los bancos establecer la legitimidad de la identidad de un cliente. Las autoridades reguladoras no son las únicas que requieren seguridad; los clientes también la esperan.

Algunos Desafíos que las Instituciones Financieras Enfrentan en la Actualidad

Los bancos conocen las numerosas formas que los defraudadores pueden intentar para robarles a ellos y sus clientes; entre ellas están los “ataques de presentación” que tratan de eludir los mecanismos de seguridad biométrica. Desafortunadamente, los intentos no se detienen ahí. Los hackers son cada vez más conocidos por crear identidades totalmente falsificadas para eludir medidas de seguridad más tradicionales en los servicios financieros. Si eso no fuera suficiente, videos e imágenes sintéticos están al alcance incluso del hacker principiante más casual.

Identidades Sintéticas

Una identidad robada es una que ha sido apropiada indebidamente de alguien – ya sea estando conectado o desconectado – de modo que un delincuente puede cometer un fraude a nombre del propietario. El ladrón de identidad podría haber conseguido información de identificación personal a través de una filtración de datos, una estafa de “suplantación de identidad”, programa espía, intrusión de redes wifi públicas, pertenencias robadas, o muchas otras formas. Sin embargo, el resultado suele ser el mismo. Los delincuentes usan su identidad robada para abrir crédito adicional, obtener préstamos, o derrochar dinero.

El fraude de identidad sintética es un método de robo más complejo. Las identidades sintéticas son identidades reales y válidas creadas por delincuentes usando credenciales falsas. Véalo como armar un rompecabezas. Cada pieza del rompecabezas es robada o falsificada, siendo luego agrupada para formar algo que ha sido legitimado. El proceso no suele ser rápido. Un delincuente puede pasar semanas creando una identidad sintética y después meses o años legitimando la identidad después de haberla creado. Pero la velocidad que le falta, la compensa con imperceptibilidad – un atributo atractivo para quienes no desean ser atrapados.

Algunas veces los adultos mayores se sienten menos cómodos con la tecnología y confían más en las personas y son víctimas comunes. Y los niños, cuyo historial crediticio suele ser "limpio" y no supervisado, también pueden ser objetivos de estos ataques. Más de 1.25 millones de niños fueron víctimas de robo de identidad en el 2021, de acuerdo con un estudio realizado por Javelin Strategy & Research.

La biometría facial se puede utilizar para ayudar a proteger un proceso de incorporación móvil contra el uso de identidades sintéticas. Pero sin la detección de prueba de vida – un proceso que determina si un usuario es una persona viva y no una máscara o un ataque de presentación similar - un defraudador podría usar una foto o video de alguien más o una "selfie" en donde su rostro esté parcialmente obscurecido, haciendo que la detección de prueba de vida sea un componente clave para proteger los procesos de incorporación y autorización de las instituciones financieras.

Deepfakes

Si pasa tiempo en las redes sociales, es posible que se haya encontrado con lo que es un avance tecnológico potencialmente preocupante – el deepfake. Las imágenes de deepfake pueden verse como algo que pasa de ser entretenido a preocupante – o incluso aterrador. Una figura política difundiendo propaganda que realmente no difundió. Un personaje histórico dando un discurso que en realidad no dió. Un actor famoso haciendo o diciendo cosas que no hizo o dijo.

La frase "deepfake" proviene de la combinación de los términos "deep learning" [aprendizaje profundo] y "fake" [falso]. A pesar de que no tiene una definición convenida universalmente, un deepfake generalmente significa que una persona en un video existente es reemplazada con el parecido de alguien más. En esencia, un deepfake es una foto, audio, o video que ha sido manipulado por Aprendizaje Automático (Machine Learning) (ML) e Inteligencia Artificial (IA) para hacer que parezca ser algo que no es.

Los deepfakes no son videos que han sido modificados con un software de edición de video. Las aplicaciones o algoritmos especializados normalmente los generan combinando videos antiguos y recientemente producidos. Estas aplicaciones de deepfake, basadas en el aprendizaje automático, desmontan los rasgos sutiles del rostro de alguien y aprenden a manipularlos en función de las condiciones individuales del video. Esas manipulaciones pueden integrarse entonces en un segundo video, haciendo una creación completamente nueva.

Los resultados son un video sintético que podría usarse con buena o mala intención. Cuando se considera un video sintético, no es difícil imaginar por qué puede ser peligroso. Existe el riesgo obvio de que las palabras o acciones sintéticas de una persona podrían incitar a alguien a hacer algo malo o peligroso. Sin embargo, un riesgo adicional es que los videos sintéticos podrían empezar a socavar la credibilidad de los videos genuinos. Los expertos en privacidad están comprensiblemente preocupados de que un deepfake podría usarse para difundir información falsa en las redes sociales o para eludir las medidas de seguridad destinadas a pillar a personas malintencionadas en la industria de servicios financieros realizando actividades como crear cuentas o accediendo a fondos.

Banca Móvil Segura –
Una Oportunidad y un Requisito

Otras Amenazas en Desarrollo

Las preocupaciones no se detienen en los deepfakes. Las transformaciones son un tipo de método de ataque biométrico que combinan los rostros de dos o más personas en un único rostro. Debido a que puede haber elementos de un usuario autorizado y el rostro de un usuario no autorizado en la transformación, la tecnología de reconocimiento facial menos robusta podría ser engañada para autorizar un acceso fraudulento. Las transformaciones se pueden usar también para falsificar documentos de identidad, como pasaportes, para personas que no pueden obtener uno legalmente, cruzar fronteras, o abrir cuentas bancarias. En este caso, se crearía una transformación combinando el parecido de la persona que no puede obtener un pasaporte con una persona que sí puede. Esta imagen transformada podría usarse entonces para obtener un pasaporte nuevo. Una vez que se recibe el pasaporte, la persona no autorizada podría usarlo para hacer "legítimamente" cualquier cosa. desde burlar la seguridad en las fronteras hasta abrir una cuenta bancaria.

En los servicios financieros, el fraude, el robo de identidad y la autenticación / verificación no autorizada son riesgos constantes. Las instituciones de servicios financieros sopesan la necesidad de mantener alejadas a las personas malintencionadas mientras proporcionan el acceso básico que sus clientes y empleados necesitan. La dificultad está en garantizar una experiencia sin complicaciones para las partes interesadas. pero presentando un muro inamovible para los delincuentes. En términos generales, los requisitos internos de seguridad en la banca móvil y los servicios financieros se dividen en dos áreas principales – la incorporación y la autenticación.

Incorporación y Autenticación Financieras Tradicionales

La incorporación es el proceso a través del cual las personas comienzan su experiencia como un cliente y normalmente es el punto en el que abren una cuenta nueva. Posteriormente, la autenticación significa cualquier momento en que un cliente necesite acceder a su cuenta para mover dinero o hacer una modificación. Desde siempre, la incorporación y el acceso a una cuenta han sido procesos presenciales, requiriendo que un cuentahabiente visite una sucursal local. El representante en la sucursal verifica entonces la identidad de la persona frente a frente y atiende las necesidades específicas del cliente. Con la expansión de la internet y los smartphones, estos requisitos presenciales cambiaron a soluciones de mayor movilidad que pueden realizarse en línea. Hoy en día, la mayoría de las instituciones financieras ofrecen a sus clientes un medio para realizar transacciones en línea o desde un dispositivo móvil. Sin embargo, las instituciones financieras tienen que trabajar mucho para mantener satisfechos a sus clientes.

Un proceso de incorporación muy largo o complicado disuade a posibles clientes. Los clientes esperan

tener una experiencia de incorporación rápida y sin problemas y no esperan tener esa experiencia en persona; tiene que ser digital.

Los Desafíos de la Incorporación Contemporánea

Si bien la incorporación presencial es sin duda un método genuino y probado de registro de clientes, existen varios desafíos a los procedimientos actuales para las instituciones financieras, que no permiten la incorporación digital. El primero es la **inconveniencia**. Con casi la mitad de la población mundial acostumbrada ahora a realizar sus actividades desde su smartphone, el hecho de que los clientes tengan que ir a una oficina es una idea cada vez más obsoleta. Los clientes esperan poder pagar sus cuentas y escanear cheques por medio de su smartphone, así que tener que ir a una sucursal para abrir una cuenta muchas veces se presenta como una sorpresa inoportuna. El 32 por ciento de los clientes se niega incluso a comenzar una solicitud si están obligados a llevar los documentos de identificación a una sucursal.

Las experiencias de incorporación en la actualidad también **requieren mucho tiempo**. Reservar tiempo para el traslado, esperar a un representante, realizar el trámite y verificar los documentos de identificación es un proceso largo que soportar para los clientes. Alrededor del 63 por ciento de los clientes han abandonado una solicitud debido al tiempo que se llevó el proceso[4], lo que representa un problema potencialmente grave para las instituciones financieras.

Otro desafío importante para los procedimientos de la incorporación contemporánea es cómo limita la capacidad de una institución de **atraer nuevos clientes**. Las poblaciones rurales representan una gran oportunidad para los bancos, pero estos clientes no siempre tienen acceso razonable a una sucursal u oficina local. Esta falta de acceso limita la posibilidad de los bancos o compañías de servicios financieros de atraer nuevos clientes. Ofrecer un proceso de incorporación móvil y seguro no sólo sería más conveniente para los clientes existentes, sino que también ayudaría a traer nuevos.

Por último, la incorporación móvil introduce requisitos normativos y un **riesgo de fraude**. Por ejemplo, un defraudador podría usar una identidad robada para abrir una cuenta falsa a nombre de la víctima. El proceso presenta riesgos para mantener la diligencia debida y obstáculos del cumplimiento normativo para el cliente. Este proceso a menudo se conoce como "conozca a su cliente," o KYC [por sus siglas en inglés] y puede tender a inhibir la capacidad del banco de ofrecer servicios bancarios sin sucursales.

Los Desafíos de la Autenticación Contemporánea

Cuando se trata de aplicaciones de banca móvil, la mayoría utiliza contraseñas para autenticar a los usuarios y dar acceso a sus cuentas. Desafortunadamente, las contraseñas ya no son un método de autenticación satisfactoriamente seguro, como lo demuestran los reportes casi diarios de nuevos casos de filtraciones de datos a gran escala o fraude generalizado. En el 2021, se encontró que el 81 por ciento de las filtraciones relacionadas con el hackeo usaron contraseñas robadas y/o débiles. Estos datos se basan en lo que la gente sabe y los hackers pueden robar ese conocimiento a través del phishing, ataques de intermediario, u otros medios.

Además, los requisitos de contraseña se han vuelto extraordinariamente complejos. Los clientes tienen que recordar frases largas que contienen caracteres tanto alfanuméricos, como no alfanuméricos. La persona promedio tiene 150 cuentas en línea que requieren una contraseña. Para recordarlas, las personas tienden a basar sus contraseñas en información que otros pueden saber fácilmente y usarlas en muchas cuentas. Así que aunque las contraseñas sean cada vez más complicadas, no son necesariamente más seguras.

El costo de los ciberataques ha afectado más al sector bancario en los últimos años, llegando a un costo promedio de $18.3 millones al año por compañía. Actualmente se estima que más del 70 por ciento de todas las filtraciones de datos tienen motivos económicos , ejerciendo cada vez más presión en los bancos y las compañías financieras para que adopten medidas que impidan que estos tipos de ataques sean exitosos. El hecho es que las contraseñas ya no son lo suficientemente seguras para proteger nuestros recursos financieros e información personal. Tanto para combatir estas amenazas, como para hacer frente a los desafíos de incorporación actuales, los datos biométricos son una solución ideal que debe considerarse.

Los Beneficios de los Datos Biométricos en la Seguridad Financiera, Incorporación y Autenticación

Para las instituciones financieras, la banca móvil se ha convertido en una forma rentable de llegar a nuevos clientes. La tecnología permite que el cliente acceda a sus cuentas bancarias desde prácticamente cualquier lugar del mundo, realice operaciones financieras en tiempo real sin ir a una sucursal y en general, tenga una comodidad sin precedentes. Los clientes han respondido bien a las soluciones móviles, con el 63 por ciento de los participantes en una encuesta diciendo que con frecuencia usan su aplicación de banca móvil.

A pesar de las reacciones positivas de los clientes y el creciente interés actual en la tecnología, las instituciones financieras han tenido hasta ahora dificultades para posicionar la tecnología de la banca móvil como su principal medio de interacción con los clientes. Esto se debe en gran medida a los muchos desafíos que las instituciones financieras enfrentan por los procedimientos de incorporación y autenticación móviles contemporáneas.

Existen varios motivos por los que los datos biométricos deberían ser una consideración primordial para los bancos y las instituciones financieras que buscan mejorar sus flujos de trabajo de incorporación y proteger sus valiosos activos durante el proceso de autenticación.

Cómo Detener los Ataques Internos

Una categoría común del fraude es cometida por una persona conocida; un miembro de la familia, amigo, o compañero de trabajo con acceso relativamente fácil a los datos de identidad de su incauto objetivo. Tratan de usarlos para hacerse pasar por su víctima ya sea para abrir una cuenta nueva a su nombre o para acceder a su cuenta existente sin su conocimiento. El reconocimiento facial hace estos tipos de ataques mucho más difíciles y la adición de tecnología biométrica de voz, los hace incluso tener menos probabilidades de ser exitosos. En cualquier caso, la detección de prueba de vida es necesaria para impedir que el perpetrador use una foto o un video de su víctima—una “suplantación”—para hacerse pasar por ella.

Una categoría menos común de fraude interno es cometida por empleados de los bancos. Aquí, un empleado recopila datos de identificación de un solicitante de cuenta como parte de su proceso de incorporación. pero después también toma una foto o un video del solicitante usando su dispositivo móvil personal. El solicitante no reconoce que esto no es parte del proceso estándar. El empleado luego usa la información de la cuenta y la imagen facial del cliente para acceder a la nueva cuenta; la línea de crédito del cliente desaparece antes de que el cliente llegue a usarla. La detección de prueba de vida también impide este tipo de ataque interno.

Incorporación Basada en Dispositivos Móviles

El reconocimiento facial y de voz son herramientas muy útiles para los procesos de incorporación de clientes nuevos y de identificación de los clientes (KYC) . Los datos biométricos modernos son cada vez más móviles, permitiendo que los clientes nuevos se registren en los servicios bancarios a través de su smartphone y eviten ir a una sucursal, lo que es particularmente conveniente en zonas rurales.

Las soluciones biométricas actuales usan las cámaras y los micrófonos de los smartphones y dispositivos móviles para realizar reconocimiento facial y de voz de

alta confiabilidad. Los documentos de identificación como licencias de conducir o pasaportes también se pueden vincular con una persona y verificar a través de "selfies" y la función biométrica en los dispositivos móviles. Al poner esta función en las manos del cliente, pueden registrarse en un sistema o autenticarse después desde prácticamente cualquier lugar, aumentando la capacidad de una compañía de atender oportunamente a sus clientes existentes y de atraer a nuevos, potencialmente reacios o que no pueden acudir a una sucursal.

En general, este proceso biométrico móvil está demostrando ser tan eficaz como si lo realizara un empleado bancario. Es una forma segura y conveniente para que los clientes confirmen su identidad sin ir a una sucursal. Y las imágenes faciales o muestras de voz se pueden usar para funciones de seguridad adicionales en el futuro.

Mayor Seguridad

Con las contraseñas siendo cada vez más un método de autenticación poco confiable, los datos biométricos se convierten en una alternativa ideal para quienes desean reforzar la seguridad. El reconocimiento facial y de voz mejoran la seguridad de acceso, al exigir al cliente que vincule su imagen facial en vivo o muestras de voz con los datos biométricos capturados durante el registro. Los datos biométricos en vivo se comparan con los datos biométricos almacenados y se permite el acceso.

Una ventaja clave es que, a diferencia de las contraseñas, los datos biométricos no se pueden robar o adivinar. Los datos biométricos usan algo único de cada persona—un rostro o voz—logrando que sea mucho más difícil de eludir para los posibles atacantes. Los datos biométricos también suelen incluir algoritmos que realizan la detección de prueba de vida para determinar si un usuario es una persona de carne y hueso y no un ataque de presentación o "suplantación" usando una foto, video, o máscara.

Con las medidas biométricas en vigor, los bancos y las empresas del sector financiero pueden estar seguros de que los clientes que sean incorporados no son impostores y que sus procedimientos de autenticación de clientes ya no son susceptibles a contraseñas propensas a fraude.

Mayor Comodidad

Abrir cuentas y realizar la autenticación son áreas donde los datos biométricos mejoran la seguridad y comodidad en los servicios financieros. En contraste con recordar una contraseña de 12 caracteres y recibir códigos de verificación por teléfono, los clientes pueden simplemente tomar una selfie cuando necesitan acceder a sus cuentas en línea.

La inclusión de los datos biométricos añade un nivel de comodidad a casi cualquier interacción con los clientes. Al ser móviles, los clientes ya no necesitan ir a una sucursal para abrir una cuenta o realizar una operación. Los datos biométricos móviles son también rápidos, realizando una vinculación de rostro y voz con la detección de prueba de vida en segundos. El proceso no tiene ninguna dificultad para los usuarios, al no requerir pasos adicionales aparte de una selfie y/o una instrucción de voz. Por último, muchas soluciones biométricas tienen configuraciones flexibles a elegir, poniendo la funcionalidad en el dispositivo o servidor para atender la disponibilidad variable de la red y proporcionando a los clientes una solución biométrica prácticamente en cualquier parte del mundo.

Los clientes han expresado su interés en usar también los datos biométricos para fines de autenticación. El 66 por ciento de las personas han usado sus datos biométricos y los consideran más fáciles y más rápidos de usar que las contraseñas tradicionales. Un estudio reveló que el 67 por ciento de los adultos de los Estados Unidos, Asia-Pacífico (APAC) y Europa se sienten cómodos usando la autenticación biométrica hoy en día, mientras que el 87 por ciento dice que se sentirán cómodos con estas tecnologías en el futuro.

El Futuro de la Banca Móvil Recae en los Datos Biométricos

Las expectativas de los clientes de sus aplicaciones de banca móvil y portales de servicios financieros siguen aumentando, particularmente mientras el mundo se convierte en un entorno sin efectivo. Esperan poder acceder a sus cuentas y realizar operaciones prácticamente en cualquier lugar sin poner en riesgo su seguridad. Debido a que son inherentemente más seguras, convenientes y flexibles que las alternativas contemporáneas, las soluciones biométricas de hoy en día proporcionan a las compañías financieras un método de verificación de identidad eficaz y elegante para cumplir con las necesidades y expectativas actuales de los clientes.

Con una mayor renuencia a salir, derivada de la COVID-19, y un aumento en los índices de robo de identidad y filtraciones de datos en todo el mundo, ahora es el momento ideal para que los bancos y las instituciones financieras consideren abordar estos desafíos, actualizando sus procedimientos de incorporación y autenticación con la tecnología biométrica. Tanto protegiendo a sus clientes existentes, como atrayendo a nuevos, los bancos y otras instituciones están considerando cada vez más los datos biométricos como una necesidad comercial y una futura realidad.

¿La interesa saber más? Visite www.aware.com

AWARE

Sources:

1 - www.bankmycell.com/blog/how-many-phones-are-in-the-world

2 - www.statista.com/statistics/1228757/online-banking-users-worldwide/

3 - javelinstrategy.com/webinar/2021-child-identity-fraud-study-key-findings

4 - www.signicat.com/battle-to-onboard

5 - www.verizon.com/business/resources/reports/dbir/

6 - blog.dashlane.com/world-password-day/

7 - www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf

8 - www.verizon.com/business/resources/reports/dbir/

9 - www.provident.bank/press-releases/provident-bank-study-shows-digital-banking-still-the-banking-method-of-choice-by-consumers

10 - https://usa.visa.com/visa-everywhere/blog/bdp/2020/01/02/banking-on-biometrics-1578003687083.html

11 - https://newsroom.ibm.com/2018-01-28-IBM-Future-of-Identity-Study-Millennials-Poised-to-Disrupt-Authentication-Landscape