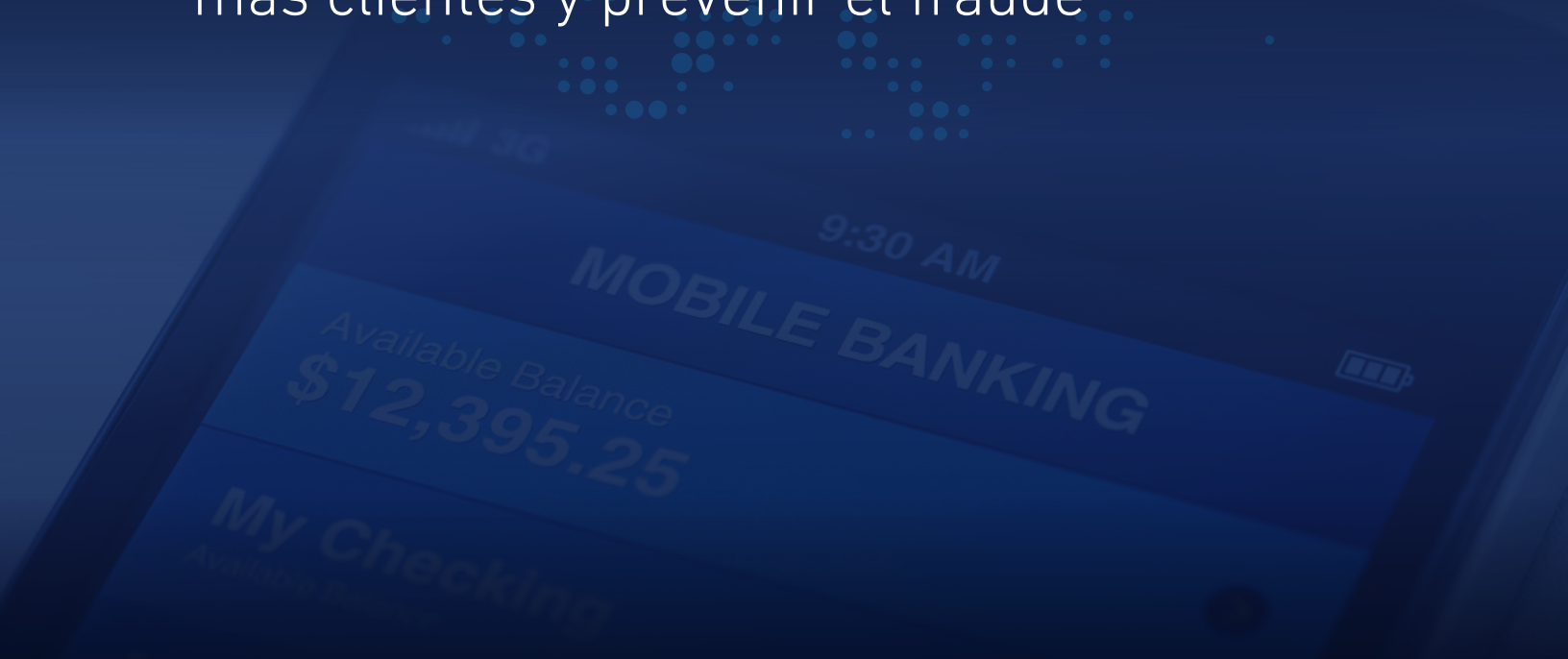
Caso de Estudio

Biometría y detección de signos vitales desde dispositivos móviles

Cómo los bancos latinoamericanos están utilizando Knomi™ para ganar más clientes y prevenir el fraude



AWARE

Introducción

Para los clientes bancarios de Aware de la región, la biometría —y, en particular, el reconocimiento facial— desempeña un papel importante en contribuir a que la banca móvil sea más accesible al hacerla más conveniente y segura.

Los enormes avances en la tecnología de dispositivos móviles y redes les brindan a los bancos la oportunidad de hacer que sus servicios sean más accesibles. Los clientes ahora pueden usar sus dispositivos móviles para solicitar rápidamente nuevas cuentas y líneas de crédito, acceder a la información de sus cuentas, y realizar compras y transacciones, todo esto sin tener que acudir a una sucursal o a un cajero automático. Los vendedores minoristas pueden emitir crédito para la compra de artículos de gran valor, como electrodomésticos, artículos electrónicos y muebles al instante, en el mismo punto de venta.

Según numerosos indicadores, América Latina es líder mundial en la adopción de la biometría para aplicaciones comerciales, y las compañías de servicios financieros contribuyen en gran medida a esta tendencia. Para los clientes bancarios de Aware de la región, la biometría —y, en particular, el reconocimiento facial— desempeña un papel importante en contribuir a que la banca móvil sea más accesible al hacerla más conveniente y segura.

En todos los casos, los bancos están utilizando la "detección de signos vitales" ofrecida como parte de la solución de autenticación biométrica desde dispositivos móviles de Aware. La detección de signos vitales se utiliza para asegurar que las imágenes faciales que se recogen son confiables por la gran variedad de controles de seguridad basados en biometría. Se aplica durante la incorporación de nuevos clientes y también para un mejor acceso a las aplicaciones móviles que utilizan autenticación biométrica.

Ejemplos de fraudesevitados por reconocimiento facial y detección de signos vitales

Los bancos de América Latina están muy familiarizados con las muchas maneras en que los estafadores pueden intentar robarles a ellos y a sus clientes; entre ellas están los "ataques de presentaciones" que intentan derribar mecanismos de seguridad biométricos. En algunos de los casos más comunes, el fraude es perpetrado no por extraños sino por familiares e, incluso, empleados. Los estafadores de carrera tienden a utilizar técnicas que son más repetitivas. En ambos casos, la biometría hace que la incorporación y la autenticación sean más resilientes al fraude, pero para ello necesitan la detección de signos vitales. A continuación se presentan algunos ejemplos de ataques de presentaciones y el papel que desempeña la detección de signos vitales.

ATAQUES INTERNOS

Una categoría común de fraude es el cometido por una persona conocida: un familiar, un amigo o un compañero de trabajo con acceso relativamente fácil a datos sobre la identidad de su blanco desprevenido. Intenta utilizarlo para usurpar la identidad de su víctima y abrir una cuenta nueva a su nombre o acceder a una cuenta existente sin su conocimiento. El uso de reconocimiento facial hace que estos tipos de ataques sean mucho más difíciles de perpetrar; y lo son aún más si se agrega la biometría de voz. En cualquiera de los casos, la detección de signos vitales es necesaria para evitar que el perpetrador use una foto o un video de su víctima para suplantarlo.

Una categoría menos común de fraude interno es el perpetrado por los empleados bancarios. Aquí, un empleado recoge datos sobre la identidad de una persona que solicita abrir una cuenta como parte del proceso de incorporación, pero también toma una foto o un video de la persona con su dispositivo móvil personal. La persona no reconoce que esto no forma parte del proceso estándar. El empleado luego usa la información de la cuenta y la imagen facial del cliente para acceder a la cuenta nueva; de este modo, la línea de crédito del cliente habrá desaparecido

mucho antes de que intente usarla. La detección de signos vitales evita este tipo de ataque interno.

IDENTIDADES SINTÉTICAS

Otra categoría de fraude involucra la creación de "identidades sintéticas" generadas y utilizadas por los estafadores para obtener crédito y préstamos que nunca planean pagar. Pueden hacer esto una y otra vez utilizando conjuntos de datos sobre identidad que son totalmente falsos o está basados en parte en una persona real. Se puede utilizar la biometría facial para ayudar a que un proceso de incorporación desde un dispositivo móvil esté protegido contra el uso de identidades sintéticas. Pero sin la detección de signos vitales, un estafador podría usar una foto o un video de otra persona o una selfi en la que el rostro está parcialmente oscurecido. Esto evita que la imagen sea utilizada por diversos mecanismos útiles de seguridad biométrica para la incorporación (vea abajo).

Cómo los bancos latinoamericanos utilizan Knomi para permitir la incorporación segura, con mínima fricción

Los nuevos clientes son un recurso esencial para el aumento de los ingresos de cualquier banco, de manera que una incorporación eficiente es una de las funciones más importantes que pueden realizar. Pero es en el proceso de incorporación de clientes cuando los bancos son más vulnerables al fraude. La incorporación es en gran medida un ejercicio de verificación de identidad a través del cual el banco intenta determinar si el potencial titular de una cuenta puede recibir una línea de crédito y se comportará como un cliente de buena fe.

Los nuevos clientes son un recurso esencial para el aumento de los ingresos de cualquier banco, de manera que una incorporación eficiente es una de las funciones más importantes que pueden realizar.

Los bancos que agregaron el software Knomi a su proceso de incorporación pueden aprovechar una selfi en vivo del solicitante para realizar diversos controles de identidad que sirven para verificar de manera positiva su identidad y detectar intentos de fraude.

Las diferentes versiones de Knomi permiten que el proceso se realice desde la aplicación móvil del banco o, de manera alternativa, desde una página web en un dispositivo móvil o una computadora de escritorio. El solicitante puede descubrir un URL en el sitio web del banco, en una publicidad por correo electrónico o en un banner publicitario. Un cliente potencial simplemente hace clic en el enlace desde su dispositivo móvil o computadora de escritorio para iniciar un proceso de solicitud en un navegador, que incluye captura de selfi en vivo. De este modo, un proceso basado en navegador y mejorado por biometría puede simultáneamente aumentar la seguridad y reducir la fricción de un proceso de incorporación que no requiere que un solicitante instale una aplicación móvil antes de efectuar la solicitud.

Los bancos latinoamericanos están utilizando el reconocimiento facial y la detección de signos vitales de Knomi para realizar diferentes controles de verificación de identidad y detección de fraude durante la incorporación de clientes. La detección de signos vitales por sí sola tiene varias finalidades valiosas:

- **Detección de intento de usurpación de identidad de una víctima objetivo utilizando "engaños"**, como fotos impresas o digitales, videos o máscaras 2D y 3D.
- **Detección de intento de ocultamiento de identidad utilizando una imagen facial de otra persona**, no humana o parcialmente oscurecida para evitar una futura detección mediante búsqueda basada en el reconocimiento facial.
- **No repudio**, que es un término que describe la capacidad de un banco de reunir evidencia admitida por un tribunal que asocia la actividad de un estafador con una persona real; esto es, evitar que el estafador niegue su participación en un intento de fraude.

Pero la detección de signos vitales también es una parte esencial de estas otras medidas de seguridad basadas en comparación y búsqueda biométricas que están siendo utilizadas por uno o más clientes de Aware de América Latina como parte de un proceso de incorporación de clientes:

- **Comparación de imagen facial con documento de identidad. Esta función**, junto con la detección de signos vitales, asegura que el documento de identidad emitido por el gobierno utilizado para proporcionar datos de identidad es auténtico y pertenece al solicitante.
- **Controles de duplicación.** Se buscan imágenes faciales de otros

clientes para asegurar que el solicitante no está intentando a escondidas tener múltiples cuentas, usar una identidad sintética o asumir la identidad de un titular de una cuenta existente.

- **Controles de listas de sospechosos.** Se realizan búsquedas de imágenes faciales de estafadores conocidos en bases de datos para asegurar que el solicitante no es un estafador conocido.
- **Controles de organismos externos.** Se pueden enviar imágenes faciales a organismos externos de aplicación de la ley para determinar si el solicitante tiene antecedentes penales.

Autenticación desde dispositivos móviles utilizando biometría confiable de la incorporación

Una vez que los clientes han sido incorporados y han abierto una cuenta, los bancos pueden utilizar la selfi tomada durante el proceso de incorporación para permitirles acceder a su cuenta de manera más segura y conveniente y realizar transacciones a través de su aplicación móvil Los clientes de Aware de América Latina han incorporado la autenticación biométrica a sus aplicaciones de banca móvil, donde se utiliza como una alternativa a las contraseñas o como un paso requerido además de las contraseñas para transacciones de mayor valor.

Como sucede con la incorporación, la detección de signos vitales es una función esencial para la autenticación biométrica mediante dispositivos móviles, ya que sin ella un estafador con acceso al teléfono de su víctima podría usar un engaño para hacerse pasar por el dueño del dispositivo y acceder a sus cuentas. La detección de signos vitales evita este ataque de presentación.

Otra manera de hacer que la autenticación biométrica sea aún más resistente a los engaños es empleando un enfoque multimodal; esto es, exigir una modalidad biométrica además del rostro, como la voz. Esto mejora en gran magnitud el rendimiento de la seguridad biométrica (menos coincidencias falsas) y la conveniencia (menos no coincidencias falsas).

Pero agregar comparación de voz y detección de signos vitales también hace que el fraude sea exponencialmente más complicado. La detección de signos vitales por voz utiliza algoritmos que detectan si una muestra de voz ha sido grabada anteriormente o ha sido generada de manera sintética. Con un enfoque de comparación de rostro solamente, el estafador necesita una falsificación de rostro exitosa para derribar la seguridad biométrica. Al combinar la modalidad de rostro y voz, el estafador también necesitará falsificar de manera exitosa la voz de la víctima, lo que es particularmente difícil, en parte debido a que las muestras de voz de las víctimas que podrían usarse para crear una falsificación son mucho más difíciles de obtener. En resumen, la biometría multimodal tiene un efecto exponencial en el rendimiento y la seguridad, lo que es particularmente útil para transacciones de alto valor.

Pero agregar comparación de voz y detección de signos vitales también hace que el fraude sea exponencialmente más complicado.

La biometría se está convirtiendo en una parte esencial de la banca móvil

Las expectativas de los consumidores en relación con la utilidad de las aplicaciones de banca móvil son cada vez mayores, en especial en lo referente a transacciones en las que no se utiliza dinero en efectivo. Sin embargo, no se espera que esta capacidad se proporcione sin sacrificar en cierta medida la seguridad. La identidad es el elemento básico de las operaciones bancarias, y la biometría es un enfoque de verificación de identidad poderoso y elegante que complementa otros mecanismos de seguridad. La biometría también ofrece un nivel de conveniencia que los consumidores han comenzado a exigir. Para muchos bancos de América Latina, la biometría es un imperativo del negocio. Tienen una visión de la biometría como una característica esencial de sus servicios y su marca. Con Knomi, Aware los está ayudando a que esta visión se convierta en realidad.