White Paper

Abordando los Nuevos Desafíos del Fraude de Identidad y Aceptando Soluciones Innovadoras

AWARE

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

Aware es un destacado proveedor global de productos y soluciones de software para la identificación y autenticación biométrica. Se utilizan para una variedad de aplicaciones, incluidos servicios financieros, seguridad empresarial, gestión de fronteras y aplicación de la ley. Aware es una empresa de capital abierto (NASDAQ: AWRE) con sede en Burlington, Massachusetts.

El Desafío de Detener el Fraude de Identidad

En la era de la creciente cantidad de transacciones digitales, el fraude de identidad se ha convertido en una amenaza persistente y en aumento con consecuencias significativas para individuos, empresas y gobiernos en todo el mundo. La proliferación de información personal identificable (PII) a través de las redes sociales y fuentes públicas, junto con el anonimato de las interacciones en línea, ha empoderado a los estafadores. A lo largo de los años, el panorama del fraude de identidad ha seguido evolucionando, lo que requiere estrategias avanzadas para combatir este problema de billones de dólares. Si bien enfoques anteriores aún pueden ser relevantes, las nuevas tecnologías y tácticas están dando forma al futuro de la prevención del fraude de identidad.

El Uso de la Biometría para Prevenir el Fraude y Proteger Identidades

El robo de identidad sigue siendo la principal causa de fraudes con motivación financiera. Con la proliferación de operaciones digitales y la facilidad de las transacciones en línea, las organizaciones criminales sofisticadas explotan las vulnerabilidades del sistema, a menudo operando más allá de los marcos legales obsoletos. Las filtraciones de datos a gran escala siguen causando incidentes frecuentes de robo de identidad significativo, muchos de los cuales permanecen sin ser detectados. El aumento del fraude de identidad sintética, donde se construyen meticulosamente identidades ficticias, presenta un desafío significativo y en rápido crecimiento.

La Biometría: Una Herramienta Crucial en la Lucha Contra el Fraude de Identidad

La integración de la detección de prueba de vida en las prácticas de seguridad convencionales se ha acelerado en los últimos años. La tecnología de reconocimiento facial incorporada en los teléfonos inteligentes se ha convertido en un estándar para el acceso seguro. Además, las capacidades de autenticación de prueba de vida en los sistemas operativos han allanado el camino para el acceso seguro a plataformas externas utilizando el reconocimiento facial, de voz e iris. La detección de prueba de vida posee atributos únicos, que constituyen una barrera efectiva contra el fraude, ofreciendo una capa adicional de seguridad más allá de los métodos de autenticación tradicionales.

Más Allá de la Autenticación: El Papel en Expansión de la Biometría

Si bien la autenticación biométrica en dispositivos personales ha ganado impulso como medida centrada en el usuario, se necesita un enfoque más integral para abordar el fraude de identidad a nivel mundial. Reconociendo las limitaciones de depender únicamente de la autenticación basada en dispositivos, los servicios de prueba y autenticación de identidad biométrica basados en la nube surgen como un camino prometedor. Este cambio tiene como objetivo abordar los diversos desafíos del fraude de identidad en varios escenarios, incluido el sector financiero, las agencias gubernamentales y los establecimientos minoristas.

El por qué:

FRAUDE DE IDENTIDAD SINTÉTICA:
La prevalencia de identidades sintéticas requiere estrategias más allá de la autenticación simple. La verificación biométrica por sí sola no aborda eficazmente esta forma de fraude.

VERIFICACIÓN DE IDENTIDAD:
La verificación biométrica confirma la identidad de la persona que se autentica, no la autenticidad de los datos de identidad en sí. Esta brecha deja espacio para establecer cuentas utilizando información fraudulenta.

PENETRACIÓN DE DISPOSITIVOS:
El uso de teléfonos inteligentes sigue en aumento y una parte sustancial de la población los utiliza regularmente. Son necesarias soluciones universales para combatir el fraude de identidad en todos los grupos demográficos.

ESTANDARIZACIÓN Y SEGURIDAD:
La autenticación en teléfonos inteligentes está limitada por la implementación del dispositivo, su sistema operativo y los proveedores de aplicaciones. La estandarización de la arquitectura y las interfaces es el objetivo de las organizaciones, pero la funcionalidad y el rendimiento biométrico no se pueden configurar universalmente en estos dispositivos. Además, estas limitaciones pueden generar problemas de seguridad para aplicaciones específicas.

Fundamentalmente, depender de contraseñas más sólidas no es suficiente para garantizar la seguridad. La seguridad sólida y la verificación de identidad confiable son necesarias para diversos tipos de cuentas, aplicaciones y entornos.

Servicios Biométricos: Un Camino Hacia la Accesibilidad Universal

La Biometría como Servicio proporciona una solución integral para prevenir el fraude de identidad, con fácil accesibilidad. Democratizan la industria al reducir costos, proporcionar gastos predecibles y fomentar la competencia entre los proveedores. Estos servicios atienden a diversas necesidades, albergan nubes, admiten diversas modalidades biométricas y transforman la industria de la verificación de identidad.

Verificación de Identidad Biométrica Salvaguardando la Integridad de los Datos

La verificación de identidad biométrica salvaguarda la integridad de los datos al verificar los datos de identidad durante la inscripción, utilizando datos biométricos y comparándolos con registros existentes. Este proceso detecta inscripciones duplicadas y evita que los estafadores creen identidades falsas, estableciendo confianza en la autenticidad de los datos biométricos inscritos y convirtiéndolo en una medida preventiva efectiva contra el fraude de identidad.

Autenticación Biométrica In-Band y Out-of-Band

La autenticación biométrica puede realizarse en el mismo canal de comunicación que la transacción (in-band) o a través de un canal separado e independiente (out-of-band). Ambos métodos brindan una seguridad mejorada, con la autenticación out-of-band agregando una capa adicional de protección a través de diversos canales de acceso.

Autenticación Basada en Dispositivo vs. Servidor

Cuando se trata de autenticación, es importante decidir si almacenar y comparar datos biométricos en el dispositivo del usuario o en un servidor central. FIDO, que es centrado en el dispositivo, realiza comparaciones en el dispositivo mismo, reduciendo el riesgo de filtraciones masivas. Sin embargo, los dispositivos robados pueden plantear riesgos de fraude. Por otro lado, el modelo centralizado en el servidor implica almacenar datos en un servidor para el control, lo que puede generar preocupaciones de confianza si se comprometen los datos biométricos. Sin embargo, falsificar biométricos es una tarea compleja, y con nuevas tecnologías y medidas contra el engaño, es complejo que los estafadores exploten brechas de seguridad biométrica.

Fortaleciendo la Prevención del Fraude de Identidad

Un banco líder en América Latina implementó la biometría para mejorar sus medidas de seguridad contra ataques vectoriales y garantizar una experiencia de autenticación de clientes sin problemas y segura. Al adoptar la biometría, evitan la inversión inicial en equipos y software de inscripción biométrica, eliminando los riesgos potenciales y los costos asociados con el mantenimiento y la obsolescencia tecnológica. Este movimiento estratégico se alinea con su compromiso de proteger las identidades y transacciones de los clientes.

La solución Aware enfatiza la importancia crítica de la verificación de identidad para establecer la identidad de las personas que solicitan nuevas cuentas y transacciones. Esto asegura que los datos biométricos recopilados sean de alta calidad y estén vinculados de manera segura a información de identidad confiable, minimizando cualquier ambigüedad o errores potenciales. El sistema admite una variedad de modalidades biométricas, incluidas las huellas dactilares, el reconocimiento facial, el iris y la voz, ofreciendo flexibilidad y opciones de seguridad integrales.

Cómo la solución Aware resolvió un ataque de inyección en un banco líder en América Latina:

INSCRIPCIÓN Y VERIFICACIÓN DE IDENTIDAD:

Al registrarse en los servicios bancarios, los clientes son dirigidos al autenticador. Durante este proceso, los clientes proporcionan pruebas de identidad de acuerdo con los requisitos del banco. Los pasos de la solución realizan la verificación de identidad y recopilan los datos biométricos necesarios. Estos datos se verifican y vinculan a la información de identidad del cliente. Cuando los clientes se inscriben en los servicios del banco, pasan por un proceso de verificación de identidad. Esto implica proporcionar pruebas de identidad y recopilar datos biométricos, que se verifican y vinculan a la información de identidad del cliente.

BÚSQUEDA Y VERIFICACIÓN EN LA BASE DE DATOS:

Los datos biométricos recopilados se almacenan de manera segura en el servidor del banco. Cuando un cliente inicia una nueva solicitud de cuenta o una transacción que requiere autenticación biométrica, el sistema busca en la base de datos las inscripciones existentes. Si surgen conflictos o inconsistencias, se desencadena una investigación adicional. Sin embargo, si la información coincide sin conflictos, se actualiza y asigna la inscripción.

AUTENTICACIÓN DE CLIENTES SIN PROBLEMAS Y COINCIDENCIA:

Los clientes pueden autenticarse fácilmente utilizando sus dispositivos móviles al enviar sus datos biométricos personales. Si la información de identidad del cliente coincide, se recupera del sistema, asegurando una identificación precisa y de confianza.

OPCIONES DE SEGURIDAD PERSONALIZABLES:

La aplicación ofrece una variedad de opciones de personalización para adaptarse a diferentes requisitos de clientes, referencias de rendimiento, preferencias de privacidad y necesidades de seguridad. Estas opciones incluyen la selección de modalidades biométricas específicas, la elección de modalidades únicas o múltiples, y la decisión de almacenar los datos biométricos en la nube privada o el servidor del banco.

EXPERIENCIA DE USUARIO PERFECTA:

La columna vertebral de la solución es una plataforma de gestión sofisticada que coordina la seguridad y los flujos de trabajo con una experiencia de usuario sin problemas.

El banco líder en América Latina ha fortalecido su infraestructura de seguridad contra ataques vectoriales, fraudes y accesos no autorizados al integrar la solución de Aware. Esto no solo aumenta la confianza del cliente a través de una verificación de identidad precisa, sino que también proporciona la flexibilidad para adaptarse a las cambiantes necesidades de seguridad y avances tecnológicos, asegurando una experiencia bancaria sólida y sin problemas para sus valiosos clientes mientras prioriza la innovación y la seguridad.

Mirando hacia el Futuro: El Futuro de la Biometría en la Prevención del Fraude de Identidad

Mientras navegamos por el complejo panorama del fraude de identidad, es evidente que la biometría ha surgido como un arma fundamental en la lucha contra esta amenaza omnipresente. Los avances en la prevención del fraude representan pasos cruciales hacia un ecosistema digital más seguro y resistente. Sin embargo, el viaje no termina aquí; más bien, continúa evolucionando a medida que la tecnología, las tácticas de fraude y las expectativas de los usuarios experimentan transformaciones.

El camino de la biometría en la prevención del fraude de identidad está lleno de oportunidades y desafíos. A medida que miramos hacia el futuro, surgen varias consideraciones clave:

INNOVACIÓN CONTINUA: El mundo de la biometría está lejos de ser estático. Las innovaciones seguirán redefiniendo lo que es posible. Desde la fusión biométrica multimodal hasta el análisis de comportamiento impulsado por la inteligencia artificial, la próxima ola de tecnologías promete soluciones aún más precisas, adaptables y amigables para el usuario.

EVOLUCIÓN DEL PANORAMA DE AMENAZAS: Los estafadores también se adaptarán. A medida que los sistemas biométricos se vuelvan más sofisticados, también lo serán los intentos de vulnerarlos. Debemos anticipar la evolución de los vectores de ataque y mantenernos adelante, mejorando no solo la fuerza de nuestras defensas, sino también la profundidad de nuestra vigilancia.

PREOCUPACIONES DE PRIVACIDAD Y ÉTICA: Con la creciente dependencia de los datos biométricos, la privacidad y la ética seguirán siendo prioritarias. Encontrar el equilibrio entre la seguridad y los derechos individuales requerirá diálogos continuos y consideraciones cuidadosas para garantizar que las soluciones biométricas sigan siendo efectivas y respetuosas de la privacidad personal.

INTEROPERABILIDAD Y ESTANDARIZACIÓN: La adopción de la biometría en todas las industrias y plataformas requiere una mayor interoperabilidad y prácticas estandarizadas. Los esfuerzos de colaboración serán fundamentales para establecer marcos cohesivos que mejoren la seguridad y reduzcan la fricción del usuario.

Próxima Generación de Dispositivos Amigables para el Usuario: El éxito de los sistemas biométricos depende de la aceptación y educación de los usuarios. Capacitar a los usuarios para que comprendan los matices de la tecnología biométrica, sus beneficios y posibles limitaciones fomentará una base de usuarios más informada y cooperativa.

REGULACIÓN Y GOBERNANZA: Los organismos reguladores de todo el mundo están trabajando con las implicaciones de la tecnología biométrica. A medida que estos marcos maduren, proporcionarán pautas esenciales para que las organizaciones aseguren el uso ético, la protección de datos y el cumplimiento de los paisajes legales en evolución.

Finalmente, a medida que continuamos abordando los desafíos del fraude de identidad y adoptando soluciones innovadoras, el papel de la biometría será fundamental. Tienen el potencial de revolucionar la forma en que autenticamos, verificamos e interactuamos en el ámbito digital. Si bien no podemos predecir todos los giros y vueltas, una cosa está clara: el camino hacia adelante implica tecnología segura, adaptabilidad y un compromiso firme con la seguridad de las identidades de individuos, empresas y gobiernos de todo el mundo.

AWARE

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