feedzai

Fraude de Cuenta Nueva

fiserv. Santander LLOYDS BANKING GROUP

El proceso de creación de una cuenta en línea puede iniciar una relación de por vida con un cliente legítimo y su institución financiera. O puede dar a los delincuentes una oportunidad para crear cuentas mula de dinero, explotar ofertas promocionales o abusar de los servicios financieros. Los estafadores utilizan información de identificación personal (PII) robada, fraude de identidad sintética y bots para cometer fraude de cuentas nuevas digitalmente. A menudo, los estafadores pueden pasar desapercibidos durante meses después de la creación de la cuenta, lo que genera pérdidas financieras graves e incluso una reprimenda regulatoria.

Detenga a los estafadores en la puerta de ingreso

Identifique aplicaciones fraudulentas

Aproveche la inteligencia de los dispositivos, la biometría del comportamiento y los datos de la red para cuantificar el riesgo de fraude. Proteja su negocio de intentos de vulneración de credenciales, identidades sintéticas, ataques de bots y cuentas mula.

Agilice los procesos de apertura de cuentas digitales

Obtenga información clara y unificada en una sola interfaz de usuario para distinguir a los solicitantes fraudulentos de los genuinos. Agilice de forma segura el proceso de creación de cuentas y genere ingresos adicionales al no rechazar a clientes genuinos.

Mejore la eficiencia operativa y reduzca costos

Aproveche los indicadores de riesgo a través de una API REST que enriquece los sistemas del resto del proceso. Tome decisiones contextuales sobre la probabilidad de apertura de una cuenta fraudulenta. La detección temprana de fraudes en el proceso de onboarding elimina los costosos pasos de verificación de identidad por parte de terceros.

Características clave

Inteligencia de dispositivos

Determine si el dispositivo ha sido rooteado (superusuario). Investigue si alguien lo usó con otras aplicaciones. Revise si el dispositivo está en alguna lista negra de dispositivos fraudulentos conocidos. Cuantifique la probabilidad de cuentas mula, identidades sintéticas o abuso de crédito en la apertura de cuentas.

Análisis de red y geolocalización

Identifique anomalías en la geolocalización y las direcciones IP en comparación con los datos de la aplicación. Detecte si alguien utilizó anteriormente la red para otras aplicaciones. Compruebe si una conexión proxy, TOR o VPN está enmascarando la red verdadera.

Monitoreo del comportamiento no humano

Identifique el uso de scripts, automatización o emulación para ataques de fuerza bruta. Detenga a los bots antes de que abran cientos de cuentas falsas en cuestión de minutos.

Cobertura web y móvil

Conozca al usuario en su canal de onboarding preferido. Implemente los SDK y los recopiladores de Javascript de Feedzai para realizar análisis de riesgos precisos en aplicaciones web y móviles.

Biometría del comportamiento

Analice los matices en cómo el titular de la cuenta interactúa con su aplicación. Los indicadores de riesgo de fraude incluyen los atajos de teclado del usuario, patrones de navegación sospechosos, fluidez en la entrada de datos y experiencia en formularios.

Premios y reconocimientos

Quadrant Knowledge Solutions — Feedzai fue distinguida como Líder en biometría del comportamiento.

datos INSIGHTS — Feedzai fue distinguida como Competidor líder en biometría del comportamiento.

FORRESTER® — Feedzai fue distinguida como Empresa de sólido desempeño en la gestión de fraudes empresariales.

¿Está todo listo para actualizar su estrategia de prevención del fraude?

Hable con un experto