LexisNexis®
RISK SOLUTIONS

CASO DE ÉXITO

LexisNexis® Risk Solutions bloquea ataques de prueba de identidad en la aplicación móvil de una cadena de restaurantes

La inteligencia de identidad digital de LexisNexis® ThreatMetrix® proporciona protección contra el abuso de incentivos y fraude de extremo a extremo para registros e inicios de sesión de aplicaciones móviles

SINOPSIS

COMPAÑÍA

Gran cadena de restaurantes estadounidense

REQUISITOS

- Detectar el abuso de incentivos ofrecidos cuando se registra una cuenta en la aplicación móvil.
- Ayudar a gestionar el problema recientemente identificado de apropiaciones de cuentas fraudulentas.
- Mantener una experiencia de aplicación móvil sin fricción para los usuarios.

SOLUCIÓN

Aprovechando la inteligencia de identidad digital de LexisNexis ThreatMetrix, esta cadena de restaurantes puede detectar y detener de manera precisa actividades fraudulentas y abusivas casi en tiempo real sin crear fricción para los usuarios legítimos.

RESULTADO FINAL

- Disminución significativa de apropiaciones de cuentas fraudulentas.
- Gran disminución del volumen de contracargos.
- Identificación precisa de usuarios que estaban abusando de incentivos gratis de nuevas cuentas.

CASO DE ÉXITO

Aprovechando la inteligencia de identidad digital de LexisNexis® ThreatMetrix®, esta cadena de restaurantes puede detectar y detener actividades fraudulentas y abusivas de manera precisa casi en tiempo real sin crear fricción para usuarios legítimos.

Resumen

Cuando esta gran cadena de restaurantes lanzó su aplicación móvil, la cual le dio la oportunidad a los clientes de evitar filas al pedir y pagar su comida en sus dispositivos móviles, quería asegurarse de que su ética honesta y centrada en el cliente se viera reflejada en línea. Sin embargo, necesitaba asegurarse de que no se abusara de sus incentivos y recompensas y que la incorporación de un método de pago en línea no expusiera a la compañía a fraudes.

Con LexisNexis® Risk Solutions, puede:

- Identificar de manera precisa circuitos fraudulentos organizados que intenten poner a prueba la identidad/credenciales de tarjetas de crédito antes de que comprometan las cuentas de usuarios fiables.
- Modificar las reglas dentro del motor de políticas de ThreatMetrix de manera rápida y simple para atacar patrones de fraude en evolución.
- Mantener la integridad de la plataforma de la aplicación móvil para usuarios recurrentes fiables.
- Continuar promoviendo con confianza ofertas e incentivos para registros de nuevas cuentas.

CASO DE ÉXITO

Problema comercial

Como incentivo para crear una cuenta en línea, esta cadena de restaurantes ofreció un producto alimenticio complementario con cada registro nuevo en la aplicación. Fijó un umbral máximo de cuentas por usuario, pero rápidamente detectó un abuso, ya que algunos clientes estaban creando múltiples cuentas desde su dispositivo para sacar provecho de esta promoción.

Aunque esto estaba afectando las ganancias de la compañía, pronto surgió un problema aún mayor como resultado de que la aplicación móvil aceptaba pagos en línea. La compañía comenzó a ver un alto volumen de intentos de apropiación fraudulenta de cuentas y contracargos, que parecían indicar una infiltración de cibercriminales organizados que estaban intentando iniciar sesión en cuentas de clientes con credenciales de identidad robadas/suplantadas y probar datos de tarjetas de crédito robadas.

Esta cadena de restaurantes necesitaba una sólida solución para el fraude que detectase de manera precisa el comportamiento anómalo o de alto riesgo al iniciar sesión y que también proporcionase una mejor visibilidad de la identidad digital verdadera del usuario para comprender si se estaba abusando de las ofertas de incentivos gratis.

El poder de la inteligencia global compartida para detectar eventos de alto riesgo casi en tiempo real

La mejor manera de abordar el cibercrimen organizado y complejo es usando el poder de una red global compartida. La LexisNexis® Digital Identity Network® recopila y procesa inteligencia global compartida de millones de interacciones diarias de consumidores, incluidos inicios de sesión, pagos y solicitudes de nuevas cuentas. Aprovechando las capacidades de LexisNexis® ThreatMetrix® y usando la información de la red Digital Identity Network, la compañía es capaz de crear una identidad digital única para cada usuario al analizar las innumerables conexiones entre los dispositivos, ubicaciones e información personal anónima. El comportamiento que se desvía de esta identidad digital fiable puede identificarse de manera precisa casi en tiempo real, alertando a esta cadena de restaurantes de abuso de incentivos y posible fraude. El comportamiento sospechoso puede detectarse e identificarse para su revisión, autenticación incremental o rechazo antes de procesar una transacción, creando una experiencia sin fricción para los usuarios fiables.

CASO DE ÉXITO

Crea identificaciones de dispositivos de validación cruzada para respaldar una detección de fraude exhaustiva en las transacciones de la aplicación móvil.

Características clave de la solución ThreatMetrix®

- **Smart ID** identifica a los usuarios recurrentes que borran las cookies, usan navegación privada y cambian otros parámetros para evitar la identificación del dispositivo. Esto mejora la detección de usuarios recurrentes y reduce los falsos positivos. Derivado del análisis de muchos navegadores, complementos y atributos de conexión TCP / IP, Smart ID detecta múltiples intentos de inicio de sesión de usuarios que intentan aprovecharse de ofertas de incentivos gratis, así como de estafadores que intentan apropiarse de cuentas de usuarios existentes.

- **Las tecnologías de análisis de conexión profunda** ofrecen una visualización más clara de los eventos sospechosos. Los estafadores a menudo se intentan esconder detrás de servicios de encubrimiento de ubicación e identidad, tales como proxies ocultos, VPNs y el navegador TOR. Con la tecnología de penetración de Proxy, la solución LexisNexis® ThreatMetrix® examina la información de cabecera del paquete TCP / IP para exponer tanto la dirección IP de Proxy como la dirección IP Verdadera.

CASO DE ÉXITO

La red LexisNexis® Digital Identity Network® recopila y procesa inteligencia global compartida de millones de interacciones diarias de consumidores, incluidos inicios de sesión, pagos y solicitudes de nuevas cuentas. Aprovechando las capacidades de LexisNexis® ThreatMetrix® y usando la información del Digital Identity Network, la compañía es capaz de crear una identidad digital única para cada usuario al analizar las innumerables conexiones entre los dispositivos, ubicaciones e información personal anónima.

LexisNexis®
RISK SOLUTIONS

Para mayor información visite:
risk.lexisnexis.com/fraude