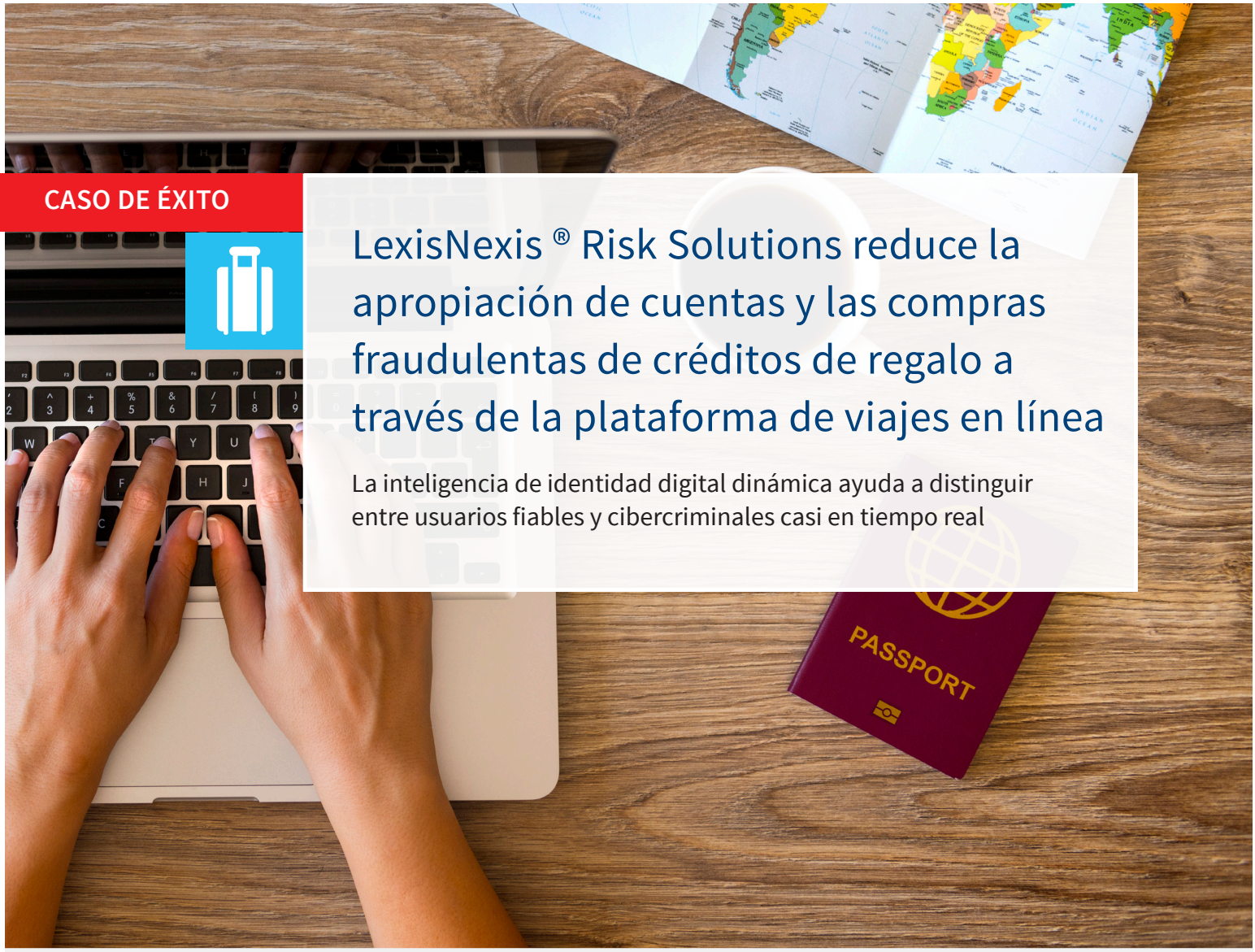
LexisNexis®
RISK SOLUTIONS



CASO DE ÉXITO

LexisNexis ® Risk Solutions reduce la apropiación de cuentas y las compras fraudulentas de créditos de regalo a través de la plataforma de viajes en línea

La inteligencia de identidad digital dinámica ayuda a distinguir entre usuarios fiables y cibercriminales casi en tiempo real

SINOPSIS

COMPAÑÍA

Plataforma de viajes en línea

REQUISITOS

- Mantener una plataforma fiable, segura y protegida para huéspedes y anfitriones.
- Proporcionar un acceso sin fricciones a servicios de reserva y pagos en línea.
- Detectar y detener de manera precisa las apropiaciones fraudulentas de cuentas.
- Evitar que cibercriminales moneticen el crédito de regalo.

SOLUCIÓN

Aprovechando la inteligencia de identidad digital dinámica de LexisNexis® ThreatMetrix® durante los eventos de inicio de sesión y pago, esta plataforma de viajes en línea puede identificar instancias de comportamiento de alto riesgo casi en tiempo real, ayudando a proteger la integridad de su comunidad.

RESULTADO FINAL

- Disminución en el número de apropiaciones fraudulentas de cuentas.
- Reducción significativa en las transacciones fraudulentas de créditos de regalo.

CASO DE ÉXITO

Resumen

El éxito de esta plataforma de viajes en línea se basa en la confianza recíproca entre los anfitriones que buscan alquilar su propiedad y los huéspedes que buscan una experiencia de viaje más auténtica. La seguridad y protección se priorizan en cada etapa del proceso del cliente, tanto en línea como fuera de línea, para evitar que los estafadores se infiltren en la comunidad en línea.

LexisNexis® Risk Solutions ayuda a identificar y detener estafadores que están intentando:

- Publicar listados falsos, transgredir cuentas o alterar los detalles de cuentas de usuarios fiables.
- Monetizar el crédito de regalo digital usando tarjetas de crédito robadas.
- Embaucar a huéspedes para que giren dinero directamente a una cuenta bancaria fraudulenta en lugar de a través de la plataforma de pago.

CASO DE ÉXITO

Problema comercial

A medida que las plataformas en línea proliferan, también lo hacen los cibercriminales que buscan aprovechar la oportunidad de ganar dinero usando credenciales robadas o a través de ataques de ingeniería social intentando estafar a clientes incautos. Como sucede con todas las plataformas de comercio electrónico y en línea, los estafadores se enfocan en esta plataforma de viajes en línea para apropiarse de cuentas valiosas o beneficiarse a través de diversas estafas o fraudes de pagos. Al cambiar la información del listado y atraer a huéspedes incautos a transferir dinero fuera de la plataforma de pago segura, los estafadores pueden beneficiarse de manera significativa.

Como sucede con muchos negocios en línea, esta plataforma quiso ofrecer de manera segura crédito de regalo digital. Sin embargo, esto se convirtió en un semillero para las actividades fraudulentas. Los estafadores estaban usando tarjetas de crédito robadas para comprar créditos de regalo e intentar ganar dinero al venderlos en otras plataformas en línea o a través de un comportamiento colusorio de reservas. Ambos casos resultaron en altas instancias de revisión manual y riesgo financiero innecesario.

La compañía necesitaba una solución para fraudes que pudiera ayudar a detectar el comportamiento anómalo y de alto riesgo al iniciar sesión, así como proporcionar una mejor visibilidad de una firma digital del usuario para comprender claramente los eventos de pago fraudulentos.

Aprovechando 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 red LexisNexis® Digital Identity Network® recopila y procesa inteligencia global compartida de millones de interacciones diarias de consumidores incluyendo 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 las compañías de posibles fraudes. El comportamiento sospechoso puede detectarse e identificarse para su revisión, autenticación incremental o rechazo antes de procesar una transacción, minimizando la fricción para la vasta mayoría de buenos usuarios en la comunidad de la plataforma de viajes en línea.

La mejor manera de abordar el cibercrimen organizado y complejo es usando el poder de una red global compartida.

Usando ThreatMetrix Smart ID para detectar dispositivos sospechosos

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, por ejemplo, de estafadores que intentan apropiarse de cuentas existentes.

Enfocando el comportamiento fraudulento en línea

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, LexisNexis® Risk Solutions 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 incluyendo 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.

LexisNexis®
RISK SOLUTIONS

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