

CASO DE ÉXITO



Una empresa global de investigación de mercado reduce el fraude previniendo la apertura de cuentas ilegítimas

La inteligencia dinámica compartida permite diferenciar con precisión entre estafadores y encuestados legítimos casi en tiempo real

Sinopsis

EMPRESA

Empresa global de investigación de mercados

REQUISITOS

- Detectar cuentas nuevas fraudulentas que se abren en nombre de encuestados.
- Proteger la integridad de los datos de las encuestas.
- Reducir las pérdidas por fraude.

SOLUCIÓN

Al emplear la inteligencia global anonimizada que aporta LexisNexis® Digital Identity Network®, una empresa global de investigación de mercados puede detectar con precisión la apertura de cuentas fraudulentas casi en tiempo real. Los datos de identidad y de pago se validan en el momento en que se realiza la transacción, lo que disminuye las complicaciones y asegura los ingresos a largo plazo.

RESULTADO

- La empresa puede continuar brindando con plena confianza servicios de encuesta inigualables a sus clientes.
- Se preservan la calidad, precisión, y legitimidad de los datos de las encuestas.
- Se reducen las pérdidas por fraude mediante la detección precisa de las inscripciones fraudulentas.

La empresa necesitaba una respuesta integral y exhaustiva para la creciente tendencia del fraude y, al mismo tiempo, mantener su buena reputación y reducir las complicaciones para los encuestados legítimos.

Resumen

Esta compañía es la principal proveedora global de soluciones de datos y tecnología para investigación de encuestas sobre consumidores y empresas. La firma se pone en contacto con los participantes de los distintos países a través de servicios de Internet, teléfono, móviles/inalámbricos y de acceso mixto. Ofrece servicios de muestreo, recopilación y procesamiento de datos, asesoramiento para diseño de cuestionarios e informes personalizados en línea. Dada la presencia global de la empresa, el riesgo de fraude es alto, ya que tanto estafadores aislados como redes delictivas organizadas buscan monetizar información fraudulenta de encuestas. La empresa necesitaba una respuesta integral y exhaustiva para la creciente tendencia del fraude y, al mismo tiempo, mantener su buena reputación y reducir las complicaciones para los encuestados legítimos.

Con LexisNexis® Risk Solutions, la empresa logró lo siguiente:

- Empleó la inteligencia global compartida de LexisNexis® Digital Identity Network® para detectar con precisión a los encuestados fraudulentos.
- Redujo el pago de incentivos fraudulentos.
- Verificó que no se rechazaran encuestados legítimos.
- Protegió la reputación de la marca y redujo las pérdidas por fraude garantizando que solo los encuestados legítimos aportaran datos.



Problema comercial

La empresa observaba datos incoherentes en las encuestas y pagos de incentivos extraordinariamente altos. Tras una investigación, se determinó que había ciberdelincuentes que completaban las encuestas para aprovechar los incentivos monetarios. Los ciberdelincuentes abrían cuentas nuevas para completar las encuestas con datos falsos, extraían los incentivos económicos y luego volvían a iniciar sesión en las cuentas existentes para obtener más recompensas. Además, se aprovechaban de las funcionalidades de investigación de mercado multimodales ofrecidas por la empresa y recopilaban datos de varias fuentes, por ejemplo aplicaciones móviles y web.

La plataforma flexible de la compañía también permitía que los ciberdelincuentes volvieran a participar para recibir todos los incentivos posibles iniciando sesión nuevamente en los sitios web. Los ciberdelincuentes pusieron en peligro la reputación de la marca empresarial, ya que sus clientes dependían de datos precisos para tomar mejores decisiones en sus compañías.

Garantice encuestas con resultados precisos utilizando LexisNexis® ThreatMetrix®

Uno de los principales requisitos empresariales de la compañía era garantizar que la solución de seguridad antifraude que se eligiera no fuera demasiado rigurosa y no disuadiera a los encuestados legítimos. ThreatMetrix eliminó la fricción en el procedimiento de inicio de sesión ya que los encuestados se autentican de forma pasiva y casi en tiempo real, sin afectar la capacidad de detectar conductas de alto riesgo típicas de los fraudes.

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

La mejor manera de afrontar los delitos cibernéticos organizados y complejos es recurrir al poder de una red global compartida. La red LexisNexis® Digital Identity Network® recopila y procesa la inteligencia global compartida aportada por millones de interacciones diarias con consumidores, incluyendo inicios de sesión, pagos y solicitudes de apertura de cuentas. Al aprovechar las funcionalidades del producto LexisNexis ThreatMetrix y utilizar información de la red Digital Identity Network, la empresa puede crear una identidad digital exclusiva para cada usuario analizando los innumerables vínculos entre dispositivos, ubicaciones e información personal

anonimizada. Las conductas que no coinciden con esa identidad digital confiable se reconocen con precisión casi en tiempo real, lo que advierte a la empresa sobre la posibilidad de fraude. Los comportamientos sospechosos se pueden detectar y marcar para revisión, autenticación adicional o rechazo antes de procesar cualquier transacción, con lo cual los usuarios legítimos tienen una experiencia sin fricción.

Al emplear la inteligencia global anonimizada que aporta LexisNexis® Digital Identity Network®, una empresa global de investigación de mercados puede detectar con precisión la apertura de cuentas fraudulentas casi en tiempo real.

Uso del motor de políticas de LexisNexis® ThreatMetrix® para personalizar las calificaciones de riesgo

La empresa aprovechó la flexibilidad que ofrece el motor de políticas de ThreatMetrix para personalizar las calificaciones de riesgo de modo que se adaptaran a los requisitos de sus actividades comerciales globales. Se incorporaron otras reglas para determinados ataques fraudulentos de mayor escala en ubicaciones geográficas específicas, sin modificar la estrategia global más amplia.



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

Acerca de LexisNexis Risk Solutions

LexisNexis Risk Solutions aprovecha el poder de los datos y el análisis avanzado para proporcionar información que ayuda a las empresas y entidades gubernamentales a reducir el riesgo y mejorar las decisiones a fin de beneficiar a las personas en todo el mundo. Brindamos soluciones de datos y tecnología para una amplia gama de industrias, incluidos seguros, servicios financieros, atención médica y gobierno. Con sede en el área metropolitana de Atlanta, Georgia, EE.UU., tenemos oficinas en todo el mundo y somos parte del Grupo RELX (LSE: REL / NYSE: RELX), un proveedor global de información y análisis para clientes profesionales y comerciales en todas las industrias. RELX es una empresa FTSE 100 y tiene su sede en Londres. Para obtener más información, visite www.risk.lexisnexis.com y www.relx.com.

Acerca de ThreatMetrix

ThreatMetrix®, una compañía de LexisNexis® Risk Solutions, permite que la economía global crezca de manera rentable y segura. Con una visión profunda de 1,4 mil millones de identidades digitales tokenizadas, LexID® Digital ofrece la inteligencia acumulada en base a 110 millones de decisiones diarias de autenticación y confianza, para diferenciar a los clientes legítimos de los estafadores en tiempo casi real.

LexisNexis, LexID, y el logo de Knowledge Burst son marcas registradas de RELX. ThreatMetrix y Digital Identity Network son marcas registradas de ThreatMetrix, Inc. © 2020 LexisNexis Risk Solutions.

Más información en risk.lexisnexis.com/fraude. NXR14280-00-0120-ES-LA