

FALLSTUDIE



Globales Marktforschungsunternehmen verringert Betrug durch Verhinderung illegitimer neuer Konten

Dynamische shared intelligence unterscheidet genau und in Echtzeit zwischen Betrügern und legitimen Umfrageteilnehmern

AUF EINEN BLICK

UNTERNEHMEN

Globales Marktforschungsunternehmen

VORAUSSETZUNGEN

- Erkennung betrügerischer neuer Konten bei der Registrierung als Umfrageteilnehmer.
- Schutz der Integrität von Umfragedaten.
- Verringerung von Betrugsverlusten.

LÖSUNG

Durch Nutzung anonymisierter globaler Informationen vom LexisNexis® Digital Identity Network® kann ein globales Marktforschungsunternehmen jetzt betrügerische neue Kontoanfragen in Echtzeit genau erkennen. Identitäts- und Zahlungsinformationen werden bei Durchführung der Transaktion validiert, was Umstände verringert und die langfristigen Einnahmen schützt.

FAZIT

- Das Unternehmen kann seinen Kunden hervorragende Umfragefähigkeiten weiterhin sicher bieten.
- Bewahrung der Qualität, Genauigkeit und Legitimität von Umfragedaten.
- Verringerung bei Betrugsverlusten durch genaue Erkennung betrügerischer Registrierungen.

Das Unternehmen benötigte eine globale, ganzheitliche Antwort auf diesen zunehmenden Betrugstrend und musste gleichzeitig seinen guten Ruf erhalten und den Aufwand für legitime Umfrageteilnehmer verringern.

Übersicht

Das Unternehmen ist ein führender globaler Anbieter von Datenlösungen und Technologie für Verbraucher- und B2B-Umfragen. Dieses Unternehmen wendet sich an Teilnehmer in verschiedenen Ländern per Internet, Telefon, Mobilfunk und gemischte Zugangsangebote.

Es bietet Stichproben, Datensammlung, Beratung zur Gestaltung von Fragebögen, kundenspezifische Online-Berichte und Datenverarbeitung. Aufgrund der globalen Präsenz des Unternehmens ist das Betrugsrisiko hoch, da sowohl einzelne Betrüger als auch organisierte kriminelle Netzwerke versuchen, betrügerische Umfrageinformationen zu Geld zu machen. Das Unternehmen benötigte eine globale, ganzheitliche Antwort auf diesen zunehmenden Betrugstrend und musste gleichzeitig seinen guten Ruf erhalten und den Aufwand für legitime Umfrageteilnehmer verringern.



Mit LexisNexis® Risk Solutions konnte das Unternehmen:

- Globale shared intelligence vom LexisNexis® Digital Identity Network® nutzen, um betrügerische Umfrageteilnehmer genau zu erkennen.
- Betrügerische Incentive–Auszahlungen verringern.
- Sicherstellen, dass legitime Teilnehmer nicht abgeschreckt werden.
- Den Ruf der Marke schützen und Betrugsverluste durch Sicherstellung, dass nur legitime Umfrageteilnehmer Umfragedaten angeben, verringern

Geschäftsproblem

Das Unternehmen beobachtete inkonsistente Umfragedaten und ungewöhnlich hohe Incentive–Auszahlungen. Nach einer Untersuchung wurde ermittelt, dass Cyberkriminelle Umfragen ausfüllten, um monetäre Anreize zu erhalten. Cyberkriminelle registrierten neue Konten, um Umfragen mit gefälschten Daten auszufüllen und Incentive–Zahlungen zu erhalten und meldeten sich dann erneut an vorhandenen Konten an, um weitere Belohnungen zu erhalten. Cyberkriminelle nutzten außerdem die multimodalen Marktforschungsfähigkeiten des Unternehmens, wobei sie Daten von mehreren Quellen sammelten, wie solchen, die durch Anwendungen vom Mobilgerät zum Internet gesendet wurden.

Die flexible Plattform des Unternehmens ermöglichte es Cyberkriminellen außerdem, sich erneut zu beteiligen, sodass sie durch erneutes Anmelden an den Websites theoretisch so viele Incentives wie möglich erhalten konnten. Cyberkriminelle gefährdeten das Markenimage des Unternehmens, da seine Kunden auf genaue Daten vertrauten, um bessere Geschäftsentscheidungen zu treffen.

Nutzung von LexisNexis® ThreatMetrix® zur Sicherstellung genauer Umfrageergebnisse

Eine der wichtigsten geschäftlichen Anforderungen des Unternehmens bestand darin, sicherzustellen, dass eine Betrugs- und Sicherheitslösung nicht zu aggressiv agierte und keine legitimen Umfrageteilnehmer abschreckte. Die LexisNexis® ThreatMetrix®-Lösung erforderte keinen Zusatzaufwand beim Anmeldeverfahren, da Teilnehmer in Echtzeit passiv authentifiziert wurden und dennoch Hochrisikoverhalten, das auf Betrug hinweist, genau erkannt werden konnte.

Die Macht der globalen Shared Intelligence bei der Erkennung von Hochrisikoereignissen in Echtzeit

Die beste Möglichkeit beim Umgang mit komplexem, organisiertem Cyberverbrechen ist der Einsatz der Macht eines globalen, gemeinsam genutzten Netzwerks. Das LexisNexis® Digital Identity Network® sammelt und verarbeitet globale shared intelligence von Millionen täglicher Verbraucherinteraktionen wie Anmeldungen, Zahlungen und neuen Kontoanträgen. Mithilfe dieser Informationen erstellt LexisNexis® Risk Solutions eine einzigartige digitale Identität für jeden Benutzer, indem die zahlreichen Verbindungen zwischen Geräten, Orten und anonymisierten persönlichen Informationen analysiert werden.

Verhalten, das von dieser vertrauenswürdigen digitalen Identität abweicht, kann in Echtzeit genau identifiziert werden, wodurch das Unternehmen auf potenziellen Betrug hingewiesen wird. Verdächtiges Verhalten kann erkannt und für die Überprüfung, Step-up-Authentifizierung oder Ablehnung gekennzeichnet werden, bevor eine Transaktion verarbeitet wird, was für ein reibungsloses Benutzer für vertrauenswürdige Benutzer sorgt.

Durch Nutzung anonymisierter globaler Informationen vom LexisNexis® Digital Identity Network® kann ein globales Marktforschungsunternehmen jetzt betrügerische neue Kontoanfragen in Echtzeit genau erkennen.

Verwendung der LexisNexis® Risk Solutions Richtlinien-Engine zur individuellen Anpassung von Risikobewertungen

Das Unternehmen nutzte die Flexibilität der LexisNexis Risk Solutions Richtlinien-Engine, um Risikobewertungen passend für seine globalen geschäftlichen Anforderungen individuell anzupassen. Es wurden zusätzliche Regeln einbezogen, um individuelle Betrugsangriffe im großen Stil an spezifischen geografischen Orten zu behandeln, ohne die umfassendere globale Strategie zu ändern.



Wenn Sie weitere Informationen möchten, rufen Sie 866.528.0780 an oder besuchen Sie risk.lexisnexis.com/FIM-EN

Über LexisNexis Risk Solutions

LexisNexis Risk Solutions nutzt das Potenzial von Daten und hochentwickelten Analysetechniken, die wichtige Einblicke liefern, mit denen Unternehmen und staatliche Einrichtungen Risiken minimieren und bessere Entscheidungen zugunsten der Menschen rund um den Globus treffen können. Wir bieten Daten- und Technologielösungen für unterschiedliche Branchen wie Versicherungen, Finanzdienstleistungen, Gesundheitswesen und Regierungen an. Mit Sitz im Ballungsraum Atlanta, Georgia, sind wir mit Niederlassungen weltweit vertreten und Teil der RELX Group (LSE: REL/NYSE: RELX), einem weltweit führenden Anbieter von Informations- und Analyselösungen für Unternehmenskunden aus unterschiedlichsten Industriezweigen. RELX ist ein Unternehmen im FTSE 100 Index mit Sitz in London. Weitere Informationen finden Sie unter www.risk.lexisnexis.com, und www.relx.com

Über ThreatMetrix

ThreatMetrix®, A LexisNexis® Risk Solutions Company, ermöglicht der globalen Wirtschaft rentables und sicheres Wachstum ohne Kompromisse. Mit umfassenden Erkenntnissen über 1,4 Milliarden tokenisierter digitaler Identitäten liefert LexID® Digital Informationen über täglich 110 Millionen Authentifizierungs- und Vertrauensentscheidungen, um legitime Kunden in Echtzeit von Betrügern zu unterscheiden. ThreatMetrix ist von Forrester Wave™ 2017 als einziger Marktführer bei risikobasierter Authentifizierung anerkannt.

LexisNexis, LexID und das Knowledge Burst-Logo sind eingetragene Marken von RELX. ThreatMetrix und Digital Identity Network sind eingetragene Marken von ThreatMetrix, Inc. Copyright © 2019 LexisNexis Risk Solutions. NXR14088-00-0919-EN-US