LexisNexis® RISK SOLUTIONS

Lösungsbeschreibung

Erkennung und Eindämmung von Betrug in der Telekommunikation bei gleichzeitiger Verringerung der Reibungsverluste für die wahren Kunden

Business-Vorteile

- **Sichern Sie Ihre Einnahmen,** indem Sie Abonnementbetrug eindämmen und potenzielle Kriminelle identifizieren, die versuchen, sich für neue Konten anzumelden
- **Bieten Sie positive Kundenerlebnisse,** indem Sie vertrauenswürdige Benutzer erkennen
- **Unterscheiden Sie vertrauliche Muster** des Nutzerverhaltens von Anomalien und erkennen Sie potenzielle Bot-Aktivitäten oder Scams
- **Schützen Sie Ihr Unternehmen** vor Strafen, Rufschädigung und potenzieller Abwanderung, indem Sie die Konten der Kunden sichern und ihre Daten und persönlichen Informationen schützen
- **Erweitern Sie Ihr Geschäft,** indem Sie die Konversionsraten verbessern und es Verbrauchern mit geringerem Risiko ermöglichen, die Dienste problemlos in Anspruch zu nehmen
- **Beibehaltung der Benutzerfreundlichkeit** durch passive Authentifizierungstools, die nur minimale manuelle Eingaben erfordern
- **Verbesserung der Automatisierung** von Arbeitsabläufen bei Betrugsverlusten zur Optimierung der betrieblichen Effizienz

Geschäftliche Herausforderungen

Eine der größten Herausforderungen für Telekommunikations-, Mobilfunk- und Medienunternehmen besteht darin, die Self-Service-Kontoverwaltung sicherer zu machen, ohne die Effizienz zu beeinträchtigen. Die Verbraucher erwarten, dass sie Telekommunikations- und Mediendienste über Apps verwalten und Tätigkeiten wie die Änderung persönlicher Daten, Zahlungsdetails und Passwörter durchführen können, die als hochriskant gelten. Sie erwarten beispielsweise einen einfachen und sofortigen Zugriff auf Rechnungsdaten und Kaufhistorie. Durch das Angebot dieser Funktionen, die die Benutzerfreundlichkeit erhöhen, eröffnen die Betreiber auch neue Möglichkeiten für kriminelle Angriffe, die sich meist auf die sich auf das Testen von Zugangsdaten, Kontomanipulation und Sammeln von Daten.

LexisNexis® RISK SOLUTIONS

Je mehr Daten Betrüger haben, desto leichter ist es, einen erfolgreichen Betrug durchzuführen

Betrüger erhalten nach einer Datenpanne Zugang zu Daten aus dem Dark Web

Betrüger testen gestohlene Zugangsdaten (z. B. Benutzername und Passwort) mit einem Telco-Konto, um zu bestätigen, dass die Zugangsdaten verwendet werden.

Wenn es in Gebrauch ist, erhalten sie Zugang zum Konto und sammeln zusätzliche Informationen: die letzten vier Ziffern der Zahlungskarte, die letzten Einkäufe, usw.

Betrüger nutzen diese Informationen, um Betrugsstrategien zu entwickeln, indem sie vorgeben, eine legitime Institution zu sein, indem sie die echten Daten der Verbraucher validieren

Wenn man das Vertrauen der Verbraucher gewinnt, kann man sie leichter überzeugen, eine Zahlung vorzunehmen oder Geld zu überweisen, z. B. bei autorisierten Push-Payment-Betrügereien (APP)

Selbst wenn es keine direkten finanziellen Auswirkungen für das Telekommunikationsunternehmen gibt, wird das Vertrauen der Kunden beeinträchtigt und der Ruf der Marke gefährdet.

Andere Betrugsmuster, die Telekommunikations-, Mobilfunk- und Medienunternehmen betreffen

Abonnement-Betrug

Kriminelle verschaffen sich auf illegale Weise persönliche Daten und verwenden diese, um Mobilgeräte und andere Kreditdienste zu beantragen, wobei sie sich als das Opfer ausgeben. Kunden werden Opfer von Identitätsdiebstahl und Telekommunikationsanbieter von Abonnementbetrug.

Synthetische Identität

Kriminelle verwenden eine Kombination aus echten Daten und gefälschten Anmeldedaten, um gefälschte Konten zu eröffnen und betrügerische Einkäufe zu tätigen. Da die vorgetäuschte Identität nicht mit einem echten Verbraucher in Verbindung gebracht wird, sind die Opfer des synthetischen Identitätsbetrugs die Telekommunikationsanbieter.

First-party Betrug

Bei diesem Szenario werden keine Identitätsdaten missbraucht, sondern der Betrüger ist der echte Inhaber des Kontos, der den Anbieter bei der Beantragung von Dienstleistungen betrügt. Dies kann durch vorsätzliche Verschuldung oder durch Rückbuchungsprozesse geschehen.

Kontoübernahme

Hier verschaffen sich Betrüger Zugang und Kontrolle über ein echtes Konto. Sobald ein Konto kompromittiert wurde, kann ein Betrüger die Kontodaten ändern, betrügerische Vertragsanfragen stellen, nicht autorisierte Transaktionen durchführen oder andere illegale Aktivitäten vollziehen.

Missbrauch von Inhalten und Testversionen

Der kostenpflichtige Zugang zu Premium-Inhalten ist Teil der zentralen Geschäfts-strategien von Medienunternehmen. Wenn es Betrügern gelingt, sich für aufeinander-folgende kostenlose Test-versionen anzumelden oder Konten für den Weiterverkauf zu erstellen, können die finanziellen Auswirkungen erheblich sein. Auch Bot-Angriffe stellen eine Bedrohung dar, bei denen gestohlene oder gefälschte Identitäts-nachweise verwendet werden, um Zugang zu erhalten.

Nach den Daten des LexisNexis® Digital Identity Network stiegen die Bot-Angriffe in der ersten Hälfte des Jahres 2022 in der Login-Phase um

597%

weltweit in den letzten 18 Monaten.

Gemeinsame Nutzung von Passwörtern

Böswillige Versuche, ein einziges Bezahlkonto für mehrere Nutzer zu verwenden, stellen für Medienunternehmen eine zunehmende Herausforderung dar. Dies führt nicht nur zu Umsatzeinbußen, sondern birgt auch ein großes Risiko für den Datenschutz und die Sicherheit der Verbraucher. Um den Schutz der Konten zu gewährleisten, werden immer häufiger Authentifizierungs-strategien eingesetzt.

Erkennen von Telekommunikationsbetrug bei gleichzeitiger Priorisierung komfortabler und personalisierter Endkundenerfahrungen

LexisNexis® Risk Solutions bietet einen mehrschichtigen Schutz vor Betrug, der es Telekommunikationsanbietern ermöglicht, die digitale Identität ihrer Nutzer besser zu verstehen, verdächtiges Verhalten oder kompromittierte Geräte zu erkennen und betrügerisches Verhalten genauer einzudämmen.

Behavioral Intelligence hilft Telekommunikationsanbietern zu beurteilen, wie ein Kunde mit einem Gerät oder einem Kanal interagiert, und kennzeichnet anomales Verhalten, so dass Anbieter bessere Betrugsentscheidungen treffen können, die Endbenutzer unterstützen und vor Betrug schützen.

Durch die Nutzung von Crowdsourced Intelligence aus dem LexisNexis® Digital Identity Network® können Telekommunikationsunternehmen tiefe Einblicke in fast anderthalb Milliarden tokenisierte Benutzeridentitäten gewinnen und so betrügerische Anfragen für neue Konten mit gestohlenen oder synthetischen Identitäten oder die automatische Erstellung von Konten durch Botnets erkennen.

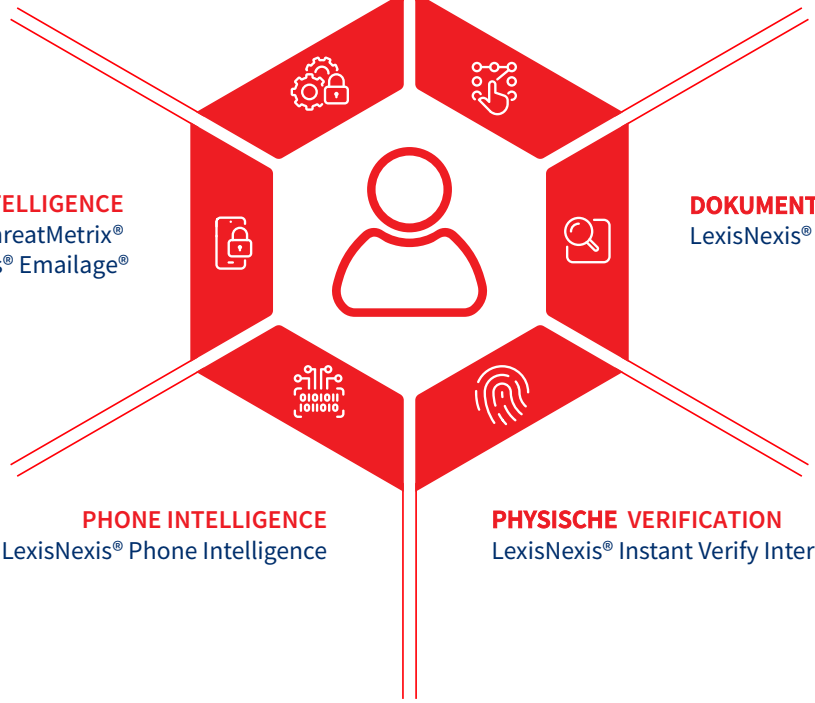
Mit einer flexiblen Sammlung von Authentifizierungswerkzeugen können Telekommunikationsanbieter das richtige Maß an Authentifizierung auf der Grundlage des von jeder Person ausgehenden Risikos anwenden. Darüber hinaus unterstützt LexisNexis® Risk Solutions Telekommunikationsunternehmen bei der Validierung von Identitätsdokumenten über mehrere Transaktionskanäle hinweg und bei der Bewertung von Verbindungen zwischen einer Telefonnummer und einer Identität, um Betrugsrisiken weiter zu reduzieren.

LexisNexis®
RISK SOLUTIONS

Robuste Funktionen zur Betrugsprävention nutzen

AUTHENTIFIZIERUNG
LexisNexis® Push-Authentifizierung LexisNexis®
Einmaliges Passwort LexisNexis® SMS OTP

VERHALTENSINTELLIGENZ
LexisNexis® Behavioral Biometrics



DIGITAL INTELLIGENCE
LexisNexis® ThreatMetrix®
LexisNexis® Emailage®

DOKUMENTEN-AUTHENTIFIZIERUNG
LexisNexis® TrueID®

PHONE INTELLIGENCE
LexisNexis® Phone Intelligence

PHYSISCHE VERIFICATION
LexisNexis® Instant Verify International

Weitere Informationen zu unseren preisgekrönten Betrugs- und Identitätslösungen finden Sie hier:

risk.lexisnexis.com

Overall **Cybersecurity Company** of the Year 2022

Best Cybersecurity Solution 2022

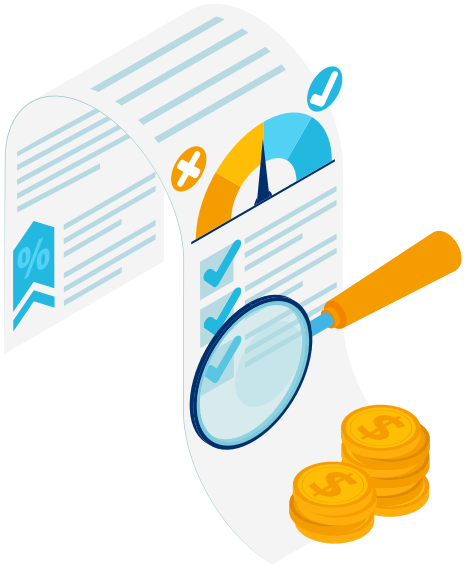
Data Initiative of the Year 2022

Best Anti-Fraud/Security Solutions Provider 2021 in the United States, Asia Pacific, Europe and Latin America

Über LexisNexis® Risk Solutions

LexisNexis® Risk Solutions macht sich die Leistungsfähigkeit von Daten und fortschrittlichen Analysen zunutze um Erkenntnisse zu gewinnen, die Unternehmen und Behörden helfen, Risiken zu reduzieren und Entscheidungen zum Wohle der Menschen rund um den Globus zu verbessern. Wir bieten Daten- und Technologielösungen für eine Vielzahl von Branchen, darunter Versicherungen, Finanzdienstleistungen, Gesundheitswesen und Behörden. Unser Hauptsitz ist in Atlanta, Georgia, und wir haben Niederlassungen auf der ganzen Welt. Wir sind Teil von RELX (LSE: REL/NYSE: RELX), einem globalen Anbieter von informationsbasierten Analyse- und Entscheidungshilfen für Geschäftskunden.

Weitere Informationen finden Sie unter www.risk.lexisnexis.com und www.relx.com.



Unsere Lösungen unterstützen Unternehmen bei Präventionsmaßnahmen gegen Finanzkriminalität, der Einhaltung gesetzlicher Vorschriften, der Reduzierung von Geschäftsrisiken, der Verbesserung der betrieblichen Effizienz und tragen zur Steigerung der Rentabilität bei.

Dieses Dokument dient rein zu Informationszwecken und ist nicht als Garantie betreffend der Funktionalität bzw. Funktionen der genannten LexisNexis Risk Solutions-Produkte zu verstehen.

LexisNexis Risk Solutions übernimmt keine Garantie für die Vollständigkeit oder Fehlerfreiheit dieses Dokuments.