LexisNexis® RISK SOLUTIONS

Solution Brief

Detect and Mitigate Fraud in Telecommunications While Reducing Friction for Good Customers

Business Benefits

- **Protect revenue** by mitigating subscription fraud and identifying potential criminals attempting to sign up for new accounts
- **Deliver positive consumer experiences** by recognizing trusted users
- **Differentiate good patterns** of user behavior from anomalies, detecting potential bot activities or instances of consumer coaching, such as scams
- **Shield your business from penalties**, reputational damage and potential churn by safeguarding consumers' accounts and protecting their data and personal information
- **Expand your business** by improving conversion rates, allowing lower risk consumers to easily onboard and use services
- **Maintain consumer convenience** with passive authentication tools that require minimal manual inputs
- **Improve automation** for fraud loss reviews and workflows, optimizing operational efficiency

Business Challenges

One of the greatest challenges that telecommunications, mobile and media companies are facing is making self-service account administration more secure without compromising efficiency. Consumers expect to manage telco and media services via apps and be able to perform activities, such as change of personal information, payment details and passwords, which are considered high risk. They expect easy and instant access to billing details and purchase history, for example. By offering these capabilities which enhance user convenience, operators also open new opportunities for criminal attacks, mostly focused on credential testing, account manipulation and data gathering.

LexisNexis® RISK SOLUTIONS

The More Data Fraudsters Have, the Easier It Is to Conduct a Successful Scam

Fraudsters get access to data from the dark web following a data breach

Fraudsters test stolen credentials (ex. Username and password) against a telco account to confirm the credentials are in utilization

If it's in utilisation, they gain access to the account and gather additional information: last four digits of the payment card, recent purchases, billing address

Fraudsters use that information to build scams strategies, pretending to be a legitimate institution by validating the consumers' genuine data

By gaining consumers' trust, it's easier to successfully convince them to make a payment or transfer money in authorized push payment (APP) scams, for example

Even when there is not a direct financial impact for the telco organization, customer trust is compromised, and the reputation of the brand is jeopardized

Other Fraud Patterns that Impact Telco, Mobile and Media Companies

Subscription Fraud

Criminals illegally obtain and use personal data to apply for mobile devices and other credit services, impersonating the victim. Customers suffer identity theft and telecommunications providers experience subscription fraud.

Synthetic Identity

Criminals use a combination of real data and fabricated credentials to open fake accounts and make fraudulent purchases. As the implied identity is not associated with a real consumer, the victims of synthetic identity fraud are the telecommunication providers.

First-party Fraud

This scenario doesn't involve any abuse of identity details, the fraudster being the genuine holder of the account who defrauds the provider in the application for services. This can be via generation of intentional debt or through chargeback processes.

Account takeover

Is where fraudsters access and gain control of a genuine account. Once an account has been compromised, a fraudster can change the account details, make fraudulent contract requests, carry out unauthorized transactions or perform other illicit activities.

Content Abuse / Free Trial Abuse

Paid access to premium content is part of the core commercial strategies for media companies. When fraudsters successfully sign up to consecutive free trials or generate accounts for reselling purposes, the financial impact can be substantial. Bot attacks also represent a threat, using stolen or spoofed identity credentials to gain access.

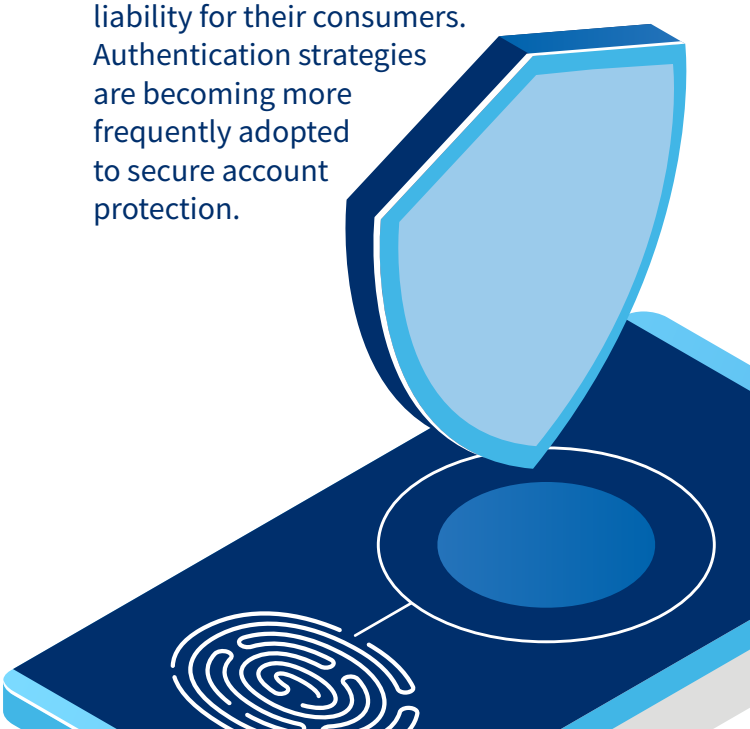
According to data from the LexisNexis® Digital Identity Network, in the first half of 2022, bot attacks at the login stage rose by

597%

globally over the past 18 months.

Password Sharing

Malicious attempts to use a single paying account for multiple users are a growing challenge for media companies. Not only does this lead to a loss of revenue, but it also carries severe privacy and security liability for their consumers. Authentication strategies are becoming more frequently adopted to secure account protection.



Detect and Mitigate Telco Fraud while Prioritizing Convenient and Personalized End User Experiences

LexisNexis® Risk Solutions delivers multiple layers of defense against fraud, enabling telecommunication providers to better understand the digital identity of their connecting users, detect suspicious behavior or compromised devices and mitigate fraudulent behavior more accurately.

Behavioral intelligence helps telcos assess how a customer is interacting with a device or a channel and flags anomalous behavior allowing providers to make better fraud decisions that support end-users and protect them from fraud.

By leveraging crowdsourced intelligence from the LexisNexis® Digital Identity Network® telcos can gain deep insight into nearly one and a half billion tokenized user identities, enabling them to detect fraudulent new account requests using stolen or synthetic identities or automated botnet account creation.

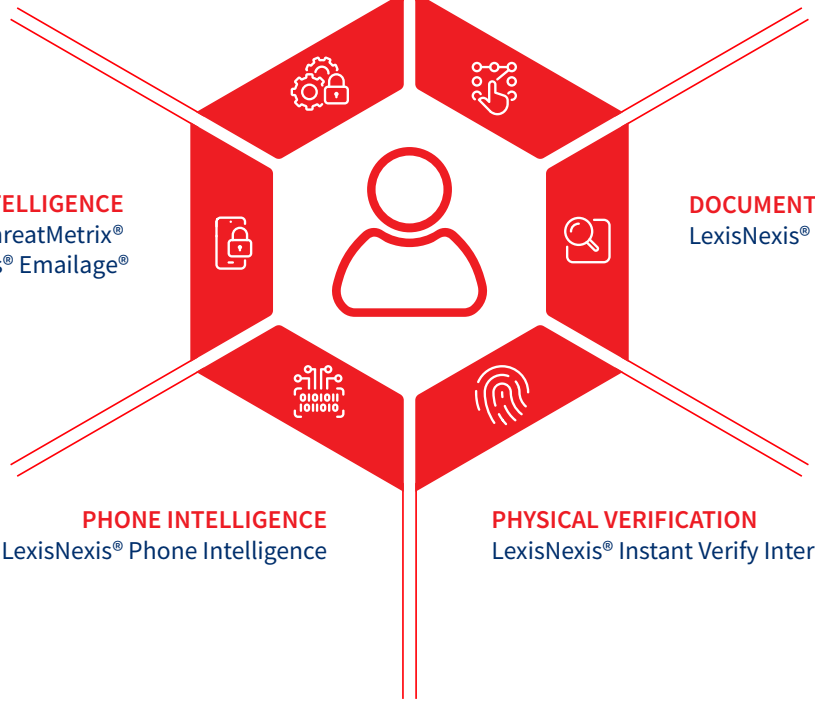
With an agile collection of authentication tools, telecommunication providers can apply the right level of authentication based on the risk presented by each individual. In addition, LexisNexis® Risk Solutions helps telcos validate identity documents across multiple transaction channels and evaluate associations between a phone number and an identity, further reducing fraud risks.

LexisNexis®
RISK SOLUTIONS

Leverage Robust Fraud Prevention Capabilities

AUTHENTICATION
LexisNexis® Push Authentication
LexisNexis® One Time Password
LexisNexis® SMS OTP

BEHAVIOR INTELLIGENCE
LexisNexis® Behavioral Biometrics



DIGITAL INTELLIGENCE
LexisNexis® ThreatMetrix®
LexisNexis® Emailage®

DOCUMENT AUTHENTICATION
LexisNexis® TrueID®

PHONE INTELLIGENCE
LexisNexis® Phone Intelligence

PHYSICAL VERIFICATION
LexisNexis® Instant Verify International

For more information on our award-winning fraud and identity solutions visit:

risk.lexisnexis.com

Overall **Cybersecurity Company** of the Year 2022

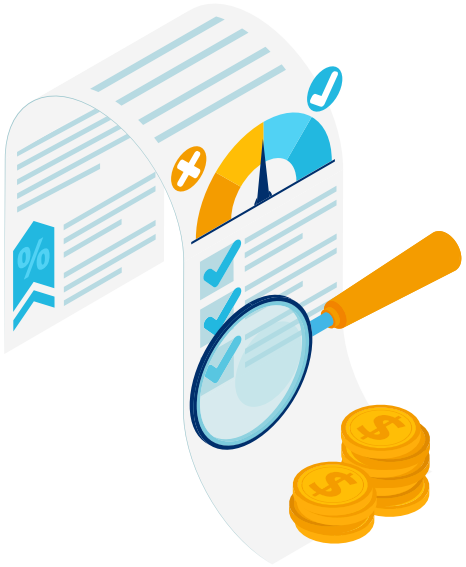
Best Cybersecurity Solution 2022

Data Initiative of the Year 2022

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

About LexisNexis Risk Solutions

LexisNexis® Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/ NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com and www.relx.com.



This document is for educational purposes only and does not guarantee the functionality or features of any LexisNexis Risk Solutions products identified. LexisNexis Risk Solutions does not warrant this document is complete or error-free.