CASE STUDY

LexisNexis® Risk Solutions Helps Detect and Block Fraud for Major Telco While Reducing Friction for Good Customers

ThreatMetrix digital identity intelligence helps differentiate fraudsters from trusted customers in near real-time

AT A GLANCE

COMPANY

Telco and media company

REQUIREMENTS

- Block high-risk behavior detected during the application process in near real time.
- Reduce friction for good customers.
- Reduce costs associated with fraud and high manual reviews.

SOLUTION

Leveraging global shared intelligence from the LexisNexis® Digital Identity Network®, this telco company was able to deploy end-to-end dynamic identity verification and authentication to better profile the legitimacy of transacting users signing up for a new mobile phone contract.

BOTTOM LINE

- Block high-risk behavior detected during the application process in near real-time.
- Reduce friction for good customers.
- Reduce costs associated with fraud and high manual reviews.

Overview

This telco is a leading player in the European market. The company embarked on extending its portfolio of services to consumers and businesses, launching a new mobile phone service offering handsets on contract and SIM-only deals, via both telesales and online.

Business Problem

As consumers continue to demand immediate communication and connectivity, adopting a mobile-first outlook, telecommunication providers are becoming increasingly burdened by fraudsters looking to capitalize on the increased distribution of mobile phones.

In launching the new mobile service, the telco recognized that it was susceptible to fraudsters looking to make money from premium handsets or defaulting on large phone bills. The company needed a solution that could accurately distinguish between legitimate and fraudulent customers in near real-time, while also promoting a frictionless experience for good, returning customers.

The telco needed to be able to detect and block fraudsters signing up for new accounts using stolen identities, as well as block cybercriminals trying to take over good user accounts to order new handsets or SIMs. The company also needed a solution which would help detect fraudulent payments and identify fraudsters attempting to monetize stolen credit card credentials. As consumer behavior becomes more complex, with fraudsters becoming increasingly adept at mirroring that behavior, it was vital for the company to genuinely understand the digital identity of its connecting users and distinguish the good from the bad.

Establishing Trusted Behavior with LexisNexis® Risk Solutions

Digital identity intelligence from LexisNexis® ThreatMetrix® enabled the operator to more accurately detect and block fraudulent applications for new mobile phones. LexisNexis Risk Solutions is integrated at key points in the application process, from when the customer first connects, to the credit agreement and payment of the mobile phone and/or contract. Leveraging digital identity intelligence, the telco was able to accurately identify high-risk and unusual behavior at new account registration. Using dynamic, behavioral history from the LexisNexis® Digital Identity Network®, the telco company was able to understand the trustworthiness of connecting users by analyzing such attributes as location, device and behavior anomalies. The telco also deployed digital identity intelligence in the second stage of the application process, using risk-based scoring to supplement additional credit verification checks. The holistic approach to detecting potentially fraudulent behavior at both new account registration and at the credit agreement, enables the telco company to detect and block potentially fraudulent behavior before a new contract is issued.

The telco further leveraged LexisNexis Risk Solutions to pinpoint fraudsters using stolen credit credentials and block fraudulent payments. Once again tapping into crowdsourced intelligence from the LexisNexis Digital Identity Network, the telco company was able to identify and block payment methods associated with prior fraudulent activity, in one instance blocking a potential fraudster using multiple credit card credentials from one device.

LexisNexis ThreatMetrix gives us the ability to paint an accurate picture of every user, capturing the unique attributes of how someone transacts online. This intelligence enabled us to significantly reduce fraud and achieve ROI within three months.

In addition, the ThreatMetrix solution was also integrated into the login page for user accounts across the telecommunication company. Good users could therefore be rated as trusted; not only does this reduce friction during the login process and protect against account takeover attacks, it also has the potential to streamline the application process for any future mobile phone contracts. The operator benefited from working collaboratively with LexisNexis® Risk Solutions, feeding back fraud data which was then immediately used to improve scores and risk assessment of transactions. By working together, fraud rejection rates were improved significantly, with referrals and false positives also reduced. In addition, the telco company was able to leverage historic data collected from transactions to see trends; new account IDs older than 60+ days from creation were found to have a low fraud rate, while pre-paid cards making initial payments were found to have a high fraud rate. These trends were used for rules optimization, further enhancing the scoring and assessment of transactions.

With LexisNexis Risk Solutions, we can leverage historic data and use our own fraud data to immediately optimize and enhance our scoring. This means that our ability to identify and detect fraud only gets stronger and stronger with each transaction.
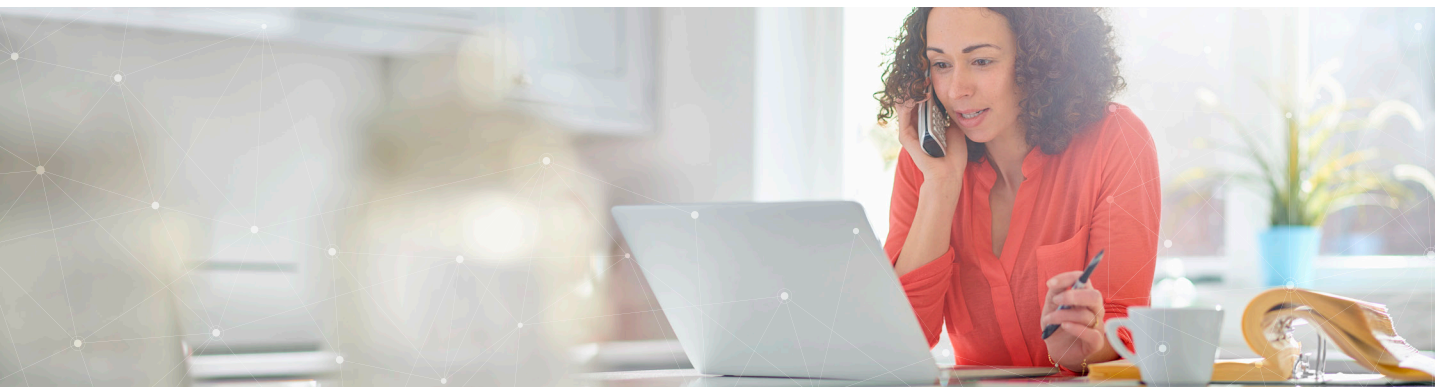
Key Features of the LexisNexis® Risk Solutions / Telco Company Partnership

- **Trust Tags** are digital labels that enable businesses to define, categorize, tag and differentiate between good and bad users, devices, locations or personas. Trust can be associated dynamically with any combination of online attributes such as devices, email addresses, card numbers or any other attributes involved in accepting, rejecting or reviewing a transaction.

- **Persona ID** helps businesses by linking current transactions to related transactions in near real-time. The rules-based mechanism links transactions via a matrix of attributes associated to the visitor, device and connection. It uncovers anomalous behavior in near real-time through the association of related historical activity.

- **Deep connection analysis technologies** give a clearer view of suspicious events. Fraudsters attempting to open a new account from an unusual or high-risk location may attempt to hide behind location and identity cloaking services such as hidden proxies, VPNs and the TOR browser. With Proxy piercing technology, LexisNexis® ThreatMetrix® examines TCP / IP packet header information to expose both the Proxy IP address and True IP address.

LexisNexis®
RISK SOLUTIONS

For more information,
call 866.528.0780 or visit risk.lexisnexis.com/FIM-EN