LexisNexis®
RISK SOLUTIONS

CASE STUDY

LexisNexis® Risk Solutions Blocks Identity Testing Attacks on Restaurant Chain's Mobile App

Dynamic digital identity intelligence provides end-to-end fraud and incentive abuse protection for mobile app registrations and logins

AT A GLANCE

COMPANY

Large U.S. restaurant chain

REQUIREMENTS

- To detect abuse of incentives offered when signing up for an account on the mobile app.
- To help manage the newly identified problem of fraudulent account takeovers.
- To maintain a friction-free mobile app experience for all users.

SOLUTION

Leveraging LexisNexis Risk Solutions dynamic digital identity intelligence, this restaurant chain can accurately detect and stop fraudulent and abusive activity in real time without creating friction for legitimate users.

BOTTOM LINE

- Significant decrease in fraudulent account takeovers.
- Large decrease in volume of chargebacks.
- Accurate identification of users who were abusing free new account incentives.

CASE STUDY

Leveraging LexisNexis® Risk Solutions dynamic digital identity intelligence, this restaurant chain can accurately detect and stop fraudulent and abusive activity in real time without creating friction for legitimate users.

Overview

When this large restaurant chain launched its mobile app, (which gave customers the opportunity to bypass lines by ordering and paying for food on their mobile devices), it wanted to ensure that its straightforward and customer-centric ethos was mirrored online. However, it needed to ensure that incentives and rewards were not abused, and that the introduction of an online payment method did not expose the company to fraud.

With LexisNexis Risk Solutions, it can:

- Accurately identify organized fraud rings attempting to test identity/credit card credentials before they compromise trusted user accounts.
- Modify rules within the LexisNexis Risk Solutions policy engine quickly and simply to tackle evolving fraud patterns.
- Maintain the integrity of the mobile app platform for trusted repeat users.
- Confidently continue to promote offers and incentives for new account registrations.

Business Problem

As an incentive to sign up for an online account, this restaurant chain offered a complementary food item with every new registration to the app. It set a maximum threshold for accounts per user, but quickly found this was being abused as customers were signing up for multiple accounts from their device to take advantage of free food.

Although this was hitting the company's bottom line, a bigger problem soon emerged as a result of the mobile app accepting online payments. The company started seeing a high volume of account takeover attempts and chargebacks, which appeared to indicate an infiltration of organized cybercriminals who were attempting to log in to customer accounts with stolen/ spoofed identity credentials, and test stolen credit card data.

This restaurant chain needed a robust fraud solution that could accurately detect anomalous or high-risk behavior at login, as well as provide better visibility into a user's true digital identity to understand whether they were abusing free incentive offers.

The Power Of Global Shared Intelligence to Detect High-Risk Events in Real Time

The best way to tackle complex, organized cybercrime is using the power of a global shared network. The LexisNexis® Digital Identity Network® collects and processes global shared intelligence from millions of daily consumer interactions including logins, payments, and new account applications. Using this information, LexisNexis® Risk Solutions creates a unique digital identity for each user by analyzing the myriad connections between devices, locations, and anonymized personal information. Behavior that deviates from this trusted digital identity can be accurately identified in real time, alerting this restaurant chain to incentive abuse and potential fraud. Suspicious behavior can be detected and flagged for review, step-up authentication or rejection before a transaction is processed, creating a frictionless experience for trusted users.

It creates cross-validation device fingerprints to support comprehensive fraud screening across mobile application transactions.

Key Features of the LexisNexis ThreatMetrix Solution

- **Smart ID** identifies returning users that wipe cookies, use private browsing, and change other parameters to bypass device fingerprinting. This improves returning user detection and reduces false positives. Derived from the analysis of many browsers, plug in, and TCP/IP connection attributes, Smart ID detects multiple sign-in attempts of user's attempting to take advantage of free incentive offers as well as fraudsters attempting to take over existing user accounts.

- **Deep connection analysis technologies** give a clearer view of suspicious events. Fraudsters often attempt to hide behind location and identity cloaking services such as hidden proxies, VPNs and the TOR browser. With Proxy piercing technology, LexisNexis® Risk Solutions examines TCP/IP packet header information to expose both the Proxy IP address and True IP address.

The LexisNexis® Digital Identity Network® collects and processes global shared intelligence from millions of daily consumer interactions including logins, payments, and new account applications. Using this information, LexisNexis Risk Solutions creates a unique digital identity for each user by analyzing the myriad connections between devices, locations, and anonymized personal information.

LexisNexis® RISK SOLUTIONS

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

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 Group (LSE: REL/NYSE: RELX), a global provider of information and analytics for professional and business customers across industries. RELX is a FTSE 100 company and is based in London. For more information, please visit www.risk.lexisnexis.com, and www.relx.com

About ThreatMetrix

ThreatMetrix®, A LexisNexis® Risk Solutions Company, empowers the global economy to grow profitably and securely without compromise. With deep insight into 1.4 billion tokenized digital identities, LexID® Digital delivers the intelligence behind 110 million daily authentication and trust decisions, to differentiate legitimate customers from fraudsters in real time. ThreatMetrix is recognized as the sole Leader in the 2017 Forrester Wave™ for risk-based authentication.

Learn more at www.threatmetrix.com.