LexisNexis® Risk Solutions Helps Global Bank Immediately Reduce Fraudulent Traffic on its Financial Exchange

LexisNexis® ThreatMetrix® dynamic digital identity intelligence blocks high velocity credentials testing, allowing a frictionless experience for legitimate customers

AT A GLANCE

COMPANY
Global Bank

REQUIREMENTS
• Accurately detect and prevent fraudulent traffic on financial exchange.
• Ensure seamless transfer of data to money management applications.
• Reduce friction for good customers.

SOLUTION
Leveraging LexisNexis ThreatMetrix dynamic digital identity intelligence, this global bank can obtain visibility into traffic on its financial exchange in near real-time, helping it block fraudulent traffic, protect user credentials, and provide a frictionless customer experience for those utilizing financial applications.

BOTTOM LINE
• Blocked 1.3 million fraudulent transactions from financial exchange.
• Accurately authenticated over 500,000 trusted users, facilitating a frictionless customer experience.
• Protected 90,000 credentials from bot attacks.
Overview

When the commercial banking division of this global bank used a financial exchange to transfer customer transaction data to money management applications, it needed to ensure that the exchange did not present new opportunities for fraudsters.

With LexisNexis® Risk Solutions, this global bank can:

• Accurately block fraudsters from testing stolen identities on its financial exchange.
• Gain clearer visibility into customer traffic on its financial exchange.
• Improve the customer experience for trusted, returning users.

Business Problem

Many businesses and consumers track their income and expenses using money management applications to help give them a comprehensive view of their finances by creating budgets, tracking and paying bills, and categorizing transactions all in one place. Customers link money management applications to their bank and credit card accounts by passing their user information through the applications. Transaction data is then transferred from the banks over the Internet via a financial exchange to the applications. Many banks use Open Financial Exchange (OFX), which is an open standard API, to provide data to financial applications such as those used for banking, stock portfolios, budgeting, and money management.

This global bank needed a fraud solution that could provide insight into activities occurring on its financial exchange and block fraudulent traffic without causing friction for legitimate customers.
When servers began crashing at this global bank, it became apparent that its financial exchange was vulnerable to fraudsters who were performing high-velocity credentials testing. Once stolen credentials are verified, fraudsters often use them to perform additional crimes or sell them on the dark web. This global bank needed a fraud solution that could provide insight into activities occurring on its financial exchange and block fraudulent traffic without causing friction for legitimate customers.

Harnessing the Power of a Global 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. Leveraging LexisNexis® ThreatMetrix® product capabilities and using information from the Digital Identity Network, the company is able to create 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 near real-time, alerting the bank to potential fraud.

Leveraging LexisNexis ThreatMetrix dynamic digital identity intelligence, this global bank can obtain visibility into traffic on its financial exchange in near real-time, helping it block fraudulent traffic, protect user credentials, and provide a frictionless customer experience for those utilizing financial applications.
Detecting Stolen Credentials and Identity Testing Attacks

As global data breaches continue to feature in the evolving cybercrime story, fraudsters have easy access to vast swaths of stolen identity credentials. They often mass test these credentials using automated bot attacks, validating and augmenting existing data to create more complete stolen identities, making it harder than ever for digital businesses to really know who they are transacting with.

LexisNexis® Risk Solutions is able to detect these credential testing attacks—even if fraudsters adjust the velocity to appear more like legitimate customer traffic—by accurately pinpointing behavioral anomalies between the digital identity of a trusted user and a fraudster:

- **LexisNexis Risk Solutions detects bot attacks** using context-based information to perform behavioral analysis of users during periods of normal operation and compares such data to that gathered during an attack, enabling the bank to differentiate between a human and a bot the moment they login/transact.

- **Deep connection analysis technologies** detect the use of technologies such as hidden proxies and VPNs and allow the bank to see the true IP address, geolocation and other attributes of each event, backed by global identity data over time.

- **Smart ID** identifies returning users that wipe cookies, use private browsing and change other parameters to bypass device fingerprinting. This improves returning user detection, reduces false positives and helps identify fraudsters who might be using the same device to make multiple payments.

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