LexisNexis®
RISK SOLUTIONS

CASE STUDY

LexisNexis® Risk Solutions Enables NewDay to Increase Fraudulent Application Detection to 70%

ThreatMetrix® Digital Identity Intelligence Helps NewDay Differentiate Good Customers from Fraudsters in Near Real Time

AT A GLANCE

COMPANY

NewDay

REQUIREMENTS

- Identify credit card applications using stolen credentials.
- Reduce revenue losses from fraudulent credit card applications.
- Reliably identify good customers from bad actors in near real time.

SOLUTION

Leveraging LexisNexis® ThreatMetrix® digital identity intelligence, NewDay can reliably detect fraudsters attempting to apply for new credit cards using stolen identity credentials that compromise good customers' established credit. NewDay can also differentiate good customers from fraudsters in near real time, reducing friction for customers utilizing their instant spend service.

BOTTOM LINE

- Successfully customized policies and models, preventing fraudsters from compromising the established credit of good customers.
- Reliably detected fraudsters at time of application, decreasing overall fraudulent applications by 70%.
- Detected evolving attack patterns as the company grew.
- Improved application process for legitimate customers.

CASE STUDY

Overview

NewDay is a major financial services company, providing millions of customers with products and services in the Near Prime and Co-Brand credit market sectors. Its proprietary risk management models and segmented approach enable them to tailor products to meet the specific needs of their customers. Some of NewDay's partners in the Co-Brand sector, which provide loyalty rewards and special offers, include established retailers such as Amazon, Debenhams, House of Fraser, Arcadia Group, and Laura Ashley. NewDay also operates three brands in the Near Prime sector – Aqua, Marbles, and Opus. NewDay's innovative credit offerings include an instant spend service in which customers can purchase credit cards online that are then instantly activated for immediate use.

By leveraging the ThreatMetrix solution, NewDay can:

- Access global shared intelligence to identify fraud by geolocation in the United Kingdom in near real time.
- Offer instant credit cards online that are available to use immediately for store purchases.
- Customize policies and models to reliably profile attackers and take immediate action.
- Leverage the ThreatMetrix Portal to identify suspicious patterns by examining links and associations, and investigating related events.
- Reduce number of fraudulent applications and time spent reviewing them.
- Reduce friction for trusted users.

"ThreatMetrix gives us access to near real time data so we can quickly make the right decisions to block fraudsters, while streamlining the application process for good customers."

—Kate Dunckley, Senior Fraud Strategy Manager, NewDay

CASE STUDY

Business Problem

As the largest non-bank card issuer, NewDay is heavily targeted by fraudsters attempting to exploit stolen identity credentials to open credit cards online. At one point, up to 70% of NewDay applications were fraudulent, making it overwhelmingly difficult to identify good customers with established credit history from fraudsters attempting to impersonate them. Relying solely on static identity verification methods such as external bureau data proved to be ineffective, as millions of credentials have been compromised in data breaches and sold on the dark web.

NewDay needed a more holistic approach to differentiate legitimate customers from fraudsters, enabling them to verify a user's true identity in near real time.

"ThreatMetrix enables us to detect fraudulent activity automatically and focus on our commitment to responsible lending and establishing long-term customer relationships."

—Kate Dunckley, Senior Fraud Strategy Manager, NewDay

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

The best way to tackle complex, global 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, the ThreatMetrix solution 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 reliably identified in near real time, alerting NewDay to 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.

"As we work with new partners, we're able to apply what we've learned from past fraudulent behaviors to customize our policies and models, making them more robust."

—Kate Dunckley, Senior Fraud Strategy Manager, NewDay

LexisNexis Risk Solutions / NewDay Partnership

- **ThreatMetrix 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, plugin, and TCP/IP connection attributes, Smart ID generates a confidence score that detects multiple fraudulent account registrations or log in attempts.
- **Deep connection analysis technologies** give NewDay 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, the ThreatMetrix solution examines TCP / IP packet header information to expose both the Proxy IP address and True IP address. These techniques help NewDay gain detailed network level signals for more reliable decision making.

CASE STUDY

- **Trust Tags** enable NewDay to differentiate between fraudsters and legitimate users. 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.

"As our organization grew and attacks evolved, we were prepared because with ThreatMetrix we had the ability to scale our solution."

—Kate Dunckley, Senior Fraud Strategy Manager, NewDay

LexisNexis® RISK SOLUTIONS

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