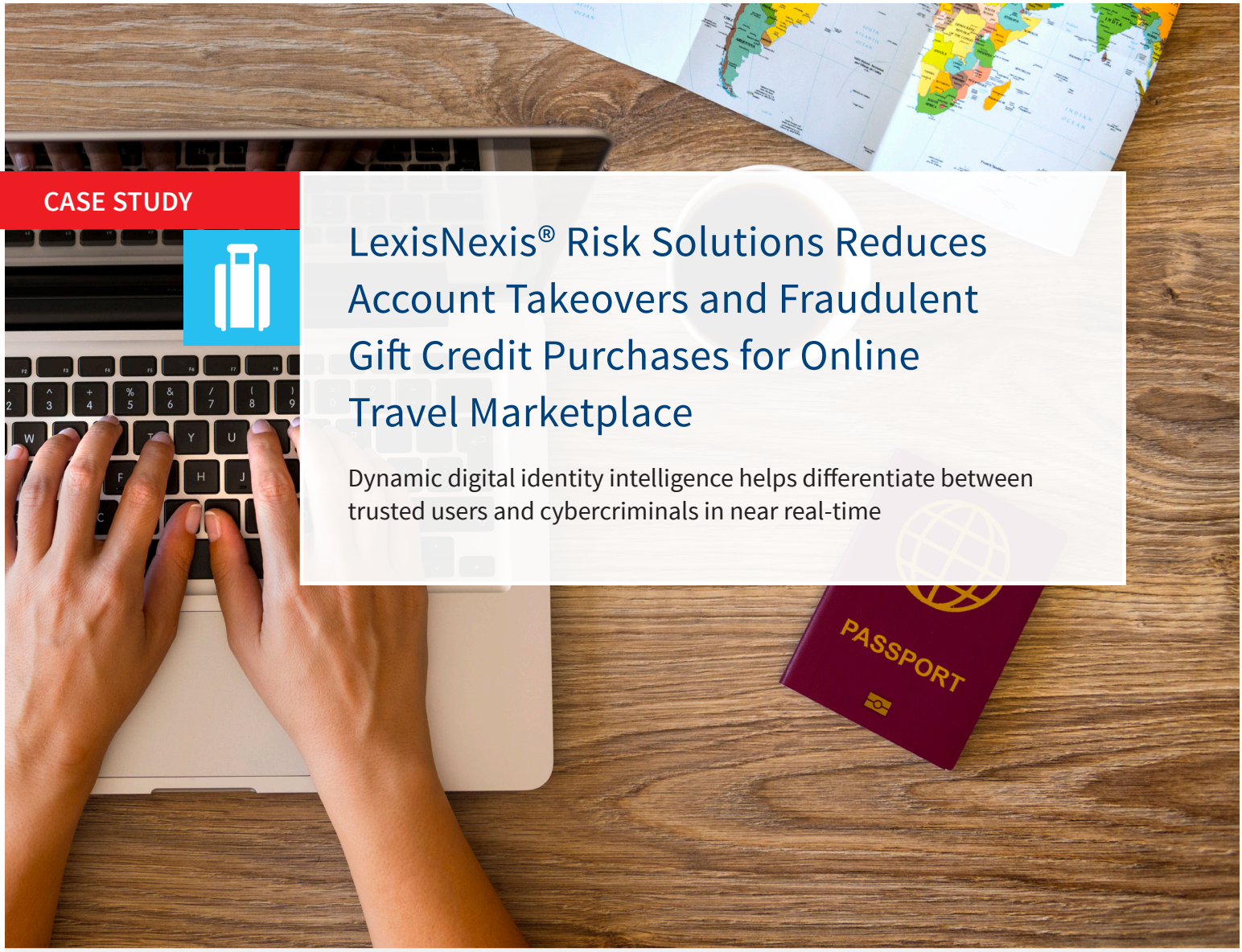
LexisNexis®
RISK SOLUTIONS



CASE STUDY

LexisNexis® Risk Solutions Reduces Account Takeovers and Fraudulent Gift Credit Purchases for Online Travel Marketplace

Dynamic digital identity intelligence helps differentiate between trusted users and cybercriminals in near real-time

AT A GLANCE

COMPANY

Online Travel Marketplace

REQUIREMENTS

- Maintain a trusted, safe, and secure platform for guests and hosts.
- Provide friction-free access to online booking and payments services.
- Accurately detect and stop account takeovers.
- Prevent cybercriminals monetizing gift credit.

SOLUTION

Leveraging LexisNexis® ThreatMetrix® dynamic digital identity intelligence during login and payment events, this online travel marketplace can identify instances of high-risk behavior in near real-time, helping it protect the integrity of its community.

BOTTOM LINE

- Decrease in number of account takeovers.
- Significant reduction in fraudulent gift credit transactions.

CASE STUDY

Overview

The success of this online travel marketplace relies on a currency of reciprocal trust between hosts looking to rent property and guests searching for a more authentic travel experience. Safety and security is prioritized at every stage of the customer journey, both online and offline, in order to prevent fraudsters infiltrating the online community.

LexisNexis® Risk Solutions helps identify and stop fraudsters who are attempting to:

- Post fake listings, compromise accounts, or alter trusted user account details.
- Monetize digital gift credit using stolen credit cards.
- Dupe guests into wiring money directly into a fraudster's bank account rather than via the payment platform.

Business Problem

As online marketplaces have proliferated, so too have cybercriminals seeking to cash in on the opportunity to make money using stolen credentials or via social engineering attacks attempting to scam unsuspecting customers. As with all ecommerce and online marketplaces, fraudsters target this online travel marketplace to take over valuable accounts or profit through various scams or payment fraud. By changing listing information and luring unsuspecting guests to wire money outside the secure payment platform, fraudsters can profit significantly.

As with many online businesses, this marketplace wanted to securely offer digital gift credit; however, this became a hotbed for fraudulent activity. Fraudsters were using stolen credit cards to buy gift credit and then attempting to make money by selling it on other online marketplaces or through collusive booking behavior. Both cases resulted in high instances of manual review and unnecessary financial risk.

The company needed a fraud solution that could help it detect anomalous and high-risk behavior at login, as well as provide better visibility into a user's digital signature to clearly understand fraudulent payment events.

Harnessing the Power of Global Shared Intelligence to Detect High-Risk Events in Near 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. 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 companies to potential fraud. Suspicious behavior can be detected and flagged for review, step-up authentication, or rejection before a transaction is processed, minimizing friction for the vast majority of good users in the online travel marketplace community.

The best way to tackle complex, organized cybercrime is using the power of a global shared network.

Using ThreatMetrix Smart ID to Detect Suspicious Devices

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, for example, fraudsters attempting to takeover existing accounts.

CASE STUDY

Shining a Light on Fraudulent Online Behavior

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. 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.

LexisNexis® RISK SOLUTIONS

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