LexisNexis®
RISK SOLUTIONS

CASE STUDY

LexisNexis® ThreatMetrix® Helps paysafecard Reduce Fraud-To-Sales Ratio By More Than 90% During Six-Year Partnership

AT A GLANCE

CUSTOMER

paysafecard

REQUIREMENTS

- Comply with anti-money laundering regulations.
- Detect fraudulent payments behavior.
- Validate legitimacy of online and offline transactions.
- Reduce fraud losses of major stakeholders.
- Manage resources effectively, cutting costs by reducing false positives.

SOLUTION

LexisNexis® ThreatMetrix® provides paysafecard with a layered defense solution, designed to enhance near real-time fraud detection and risk-decisioning amidst a constantly evolving cybercrime landscape. Combining digital and physical identity intelligence with key ThreatMetrix capabilities, such as Trust Tags and Behavioral Biometrics, enables paysafecard to detect high-risk and fraudulent payments, while recognizing more transactions as trusted across the customer journey.

paysafecard has been a long-term customer of LexisNexis® Risk Solutions, with an active relationship that has supported the development of new features and functionality, alongside internal investments in feature adoption and increased operational resourcing. Evolving in tandem, this has resulted in record-breaking success and enables paysafecard to report positively against their own, and their peer, fraud performance benchmarks.

BOTTOM LINE

- Over 90% of users now rated as trusted, dramatically reducing potential friction on the customer experience.
- Since the solution was deployed, ThreatMetrix has helped support a substantial growth in the volumes of transactions processed, which have more than doubled in six years.
- Fraud-to-sales ratio cut from 73 basis points to 2.3 basis points over six years.
- False Positive volumes reduced by approximately 70%.

Overview

paysafecard is an online payment method that allows users to pay for goods and services securely and privately at a huge range of global online merchants in 50 markets. paysafecard vouchers are sold at more than 650,000 retail outlets, gas stations and grocery stores, providing a simple, prepaid alternative to online payments. This also makes online payments more accessible to the unbanked and underbanked, negating the need for a bank account. However, paysafecard also offers customers an online account, my paysafecard, which gives users the opportunity to extend functionality to include a personal payments account to manage balances and replenish accounts.

A Challenging Fraud Landscape

With a strong market position and a large customer base, paysafecard was a key target for fraudsters looking to exploit process and data loopholes, and test fraud defenses. Re-investing the credentials stolen from high-profile data breaches, fraudsters were using these to perpetrate payment fraud.

However, despite the need to address the payment threat from fraudsters, paysafecard also recognized the need to not solely focus on the identification and use of stolen credentials, but also understand the impact on good customers. Enhancing its risk decisioning with new capabilities enabled paysafecard to promote and reward positive, trusted behavior while detecting fraudulent payments in near real time.

Leveraging this trust, paysafecard could also focus on reducing customer friction, which was another core focus of the fraud team. Paysafecard was also able to reduce the number of false positives by approximately 70 percent while growing the business at the same time. This led to happier customers while simultaneously reducing operational costs.

> "LexisNexis ThreatMetrix has delivered remarkable developments, coinciding with paysafecard deciding to intensify the invested resources into the evolution of a rules engine. As a result, we have significantly reduced fraud."
>
> — HANY RAZI, HEAD OF GLOBAL FINANCIAL CRIME INTELLIGENCE & ANALYTICS – PAYSAFE GROUP

Designing a Solution

In today's cyber landscape, single point solutions are no match for increasingly sophisticated fraudsters who are looking to maximize monetary gain and minimize detection. With LexisNexis ThreatMetrix, paysafecard gets a layered defense of fraud, identity and authentication capabilities across the entire online customer journey, executable in near real time. Capturing the unique specificities of customer behavior on a per-user basis, ThreatMetrix features such as Smart Rules, Behavioral Biometrics, Persona ID and the ThreatMetrix Mobile Software Development Kit (SDK), enable paysafecard to gain a single view of their end consumer across the entire online customer journey.

"ThreatMetrix enables us to take a surgical approach, where we can cut out malicious transactions without affecting good, healthy customers. We are now seeing the first effects and the increased value of the LexisNexis® Digital Identity Network®."

— HANY RAZI, HEAD OF GLOBAL FINANCIAL CRIME INTELLIGENCE & ANALYTICS – PAYSAFE GROUP

"We relied heavily on the Persona ID functionality for convergent behavior of customers for the first stage," says Hany Razi of Paysafe Group. "Analysis of customer behavior indicated that returning customers showed highly predictable behavior, such as purchasing our product at the same point-of-sale (POS) terminal, or the same merchant. In the next step, we tried to identify high-risk, divergent behavior utilizing the same technology. Previously unknown devices utilizing a wide range of POS terminals and entering our systems with a high-risk transaction raised our suspicions right from the start and can be identified via the ThreatMetrix solution in a reliable way."

Leveraging Knowledge with ThreatMetrix Trust Tags

A key component in paysafecard's identification of good, returning customers was the ongoing recognition of trust. Using ThreatMetrix Trust Tags, paysafecard can mark good, returning customers, and reward them with positive scores when assessing them for risk.

Trust Tags are digital labels that can be applied to various combinations of entities within a user's digital persona to indicate their trustworthiness; reducing friction for legitimate users and more reliably identifying high-risk behavior. Integrating Trust Tags into its strategies enabled paysafecard to combat fraud more effectively, increase the complexity of its rules and build better customer relationships.

"We are now using intelligence from multiple touchpoints in order to promote better decision making," says Razi. "Trust tags are used as a sort of "Dye Pack", like banks might use. High-risk events are being marked and malicious transactions can be identified and verified later on during the payment event. Once the transaction is recognized, we place a very sticky fingerprint on all identifiers used by the fraudsters, helping to combat fraud."

From Device-Based Decisioning to a Behavior-Based Approach, Enabled by ThreatMetrix Smart Rules

To ensure it was reliably differentiating between trusted and risky transactions, paysafecard used ThreatMetrix Smart Rules to create dynamic user behavior models.

"Anomalous behavior is more complex than ever, and the capability to adjust to this by having a dynamic threshold significantly impacted the way we design rules within paysafecard," says Razi. "While everything was customer-centered in the past, we can now also evaluate on a merchant/distribution level. A sharp increase of events is now very likely to be detected, while slow, steady growth does not force us to constantly change the thresholds."

> "We look forward to each product release because it's like Christmas for us. Every enhancement gives us additional layers of complexity to make better fraud decisions."
>
> — HANY RAZI, HEAD OF GLOBAL FINANCIAL CRIME INTELLIGENCE & ANALYTICS – PAYSAFE GROUP

CASE STUDY

Finding Early Success with Behavioral Biometrics

Continuing with the theme of ThreatMetrix feature adoption, paysafecard has recently implemented Behavioral Biometrics, giving the payments provider another dimension of intelligence.

Behavioral Biometrics captures how an end user interacts with a desktop, mobile or laptop device via their keyboard, mouse and/or touchscreen. Part of the ThreatMetrix solution, Behavioral Biometrics can be added as an additional layer of defense for fraud and risk decisioning across the online customer journey.

When combined with Digital Identity Intelligence, Behavioral Biometrics helps paysafecard to:

- Layer the way a user interacts with their device, with information relating to the trustworthiness, integrity and authenticity of that device.
- Detect bots mass-testing lists of identity credentials.
- Differentiate between trustworthy and high-risk users in near real time, without adding friction for good customers.
- Build trust and context around good user behavior.

"The Behavioral Biometrics features have allowed us to efficiently identify specific clusters of fraudulent accounts, as well as adding an extra layer of precision in transactional rule setting, enhancing the target on fraudulent behavior, while protecting regular customers."

— **DIANA LAPTUCA,** SENIOR MANAGER OF FINANCIAL CRIME FORENSICS – PAYSAFE GROUP

LexisNexis® RISK SOLUTIONS

For more information, visit risk.lexisnexis.com