LexisNexis®
RISK SOLUTIONS

CASE STUDY

Intelligence from LexisNexis® ThreatMetrix® Helps French Retailer Cdiscount Better Detect Fraudulent Activity Across the Customer Journey, Dramatically Reducing Account Takeovers and Payment Fraud

AT A GLANCE

CUSTOMER

Cdiscount

REQUIREMENTS

- Protect existing customers from fraudulent account takeovers.
- Accept more orders from good, trusted customers, minimizing online friction.
- Authorize various payment solutions for secure transactions.
- Detect fraudulent orders using stolen / spoofed credit cards.

SOLUTION

French retailer Cdiscount leverages digital identity intelligence from the LexisNexis® Digital Identity Network® to reliably differentiate between trusted and fraudulent online behavior in near real time. Device, location and behavior data help the retailer identify high-risk scenarios.

BOTTOM LINE

- Significant reduction in fraudulent account takeovers.
- Reliable detection of fraudulent payment attempts using stolen credit card credentials.
- Reduction of secure transactions routed via 3-D Secure (3DS) step-up authentication.
- Limiting the display of split payment to legitimate customers only.
- Detected 95% of potential fraud losses.

Overview

Since the sale of its first DVD for less than €1 in 1998, Cdiscount has continued its spirit of innovation; adapting to market changes and anticipating consumer trends, moving in to markets such as high-tech and household appliances, but also wine, home decoration, toys and even electricity.

In 2011, the company went from a classic retailer model to a platform model by opening a marketplace. This dramatically increased its product range to nearly 40 million products, representing the offering of approximately 1,000 supermarkets combined.

Cdiscount is now the leader in French eCommerce. In 2018 it turned over more than €3.6 billion, with over 20 million unique visitors and nearly 9 million customers.

Business Problem

Today, more than ever, customers are turning to eCommerce, prompting a dramatic and steady rise in online transactions.

However, online retailers are stuck between providing the smoothest possible experience for customers (new and existing) and protecting themselves from fraudsters who take advantage of the anonymity provided by digital channels.

Fraudsters continue to be masters of impersonation, cloaking themselves with genuine customer data to appear wholly convincing in an online transaction. There is no shortage of stolen data available for purchase on the dark web, and this is constantly updated with fresh pickings from the continual stream of global data breaches.

How, for example, can online retailers accurately identify a fraudster who, by creating a new account, can make a payment using stolen bank card details? Likewise, how can they ensure that fraudsters are not exploiting trusted customer accounts via a well-timed account takeover, perhaps accessing saved payment credentials undetected?

Key pressure points for Cdiscount included:

- Detecting fraudsters using stolen identity credentials, often via bots or automated scripts, to take over trusted customer accounts.
- Blocking the use of stolen credit card credentials during the online checkout process, often resulting in high levels of chargebacks.
- Ensuring that good users were not caught in the net of robust fraud detection, and forced to abandon their shopping basket in favor of a lower friction checkout experience elsewhere.

> “Our key priority is to help our good customers place orders safely, securely and without the risk of their account being compromised. By detecting fraudulent activity as early as possible in the customer journey, ThreatMetrix protects the integrity of our platform.”
>
> — Cdiscount

Building a Picture of True Digital Identity at Each Stage in the Online Journey

The design of an effective solution for Cdiscount started with being able to reliably recognize trusted, returning customers, regardless of when and where they transact. LexisNexis ThreatMetrix helps Cdiscount collate intelligence relating to the customer's device, location, online behavior and payment credentials, building up a complete digital identity of every transacting user. Not only was this intelligence harnessed from Cdiscount transactions, it was collated across all transactions relating to that user within the Digital Identity Network®.

The Digital Identity Network collects and processes millions of global transactions across thousands of websites every day, helping to piece together the digital footprint of online users across businesses, industries and locations.

This capability meant that behavior that deviated from this trusted profile could be flagged to Cdiscount in near real time, whether this was an unusual login or a transaction coming from a new location.

Leveraging Trust to Identify Account Takeover in Near Real Time

Regardless of whether a fraudster is in possession of genuine login credentials, LexisNexis ThreatMetrix could flag the fact that the transaction was coming from a new or high-risk device, an unusual location not previously associated with the trusted user, or at a velocity that was anomalous with normal human behavior (and therefore indicative of automated bot traffic).

Cdiscount could therefore block login attempts that were deemed high-risk, protecting good user accounts without imposing unnecessary friction.

> "The size and scale of the LexisNexis® Digital Identity Network® — together with the eCommerce fraud expertise from the Professional Services team — has allowed us to continually refine and improve our fraud detection policies so that regardless of what cybercriminals throw at us, we can adapt."
>
> — Cdiscount

Harnessing Global Shared Intelligence to Reliably Risk-Assess Online Payments

The ultimate endgame for a fraudster is to “cash-out” — whether by monetizing stolen credit card details via a high-value transaction, or by accessing a customer’s saved credit card to make a fraudulent purchase.

Securing the payments touchpoint was therefore a key requirement to ensure the integrity of Cdiscount’s online platform. LexisNexis ThreatMetrix helps Cdiscount risk-assess a customer transaction at pre-payment stage:

- For low-risk transactions, Cdiscount offers customers the option to split their payments across 4 installments; a popular and flexible approach to online ordering.
- High-risk transactions are pushed down the 3DS rails for step-up authentication.

High-risk scenarios that were likely indicative of a fraudster using stolen credentials could be flagged in near real time, and included:

- Instances of fraudulent accounts that had been set up solely to monetize stolen credit card credentials. This may include scenarios such as several credit cards associated with one account.
- The same digital identity trying to create several different accounts.
- A digital identity that has been marked as fraudulent in the Digital Identity Network®.
- Anomalies in comparison to a customer’s trusted order history.
- Orders placed from a geolocation considered risky or that the user was attempting to conceal.

> “Being able to harness such rich data relating to the geolocation of a transaction, combined with best-in-class device intelligence relating to each online user, is a key differentiator for us. It’s where ThreatMetrix really excels.”
>
> — Cdiscount

Identifying Payment Attempts from Automated Bots Attempting to Bypass 3DS Authentication

In addition to payment fraud using stolen credentials, Cdiscount was also experiencing attacks from automated bots operating on French IP addresses. Attacks typically involved multiple payment attempts, decreasing in value over time.

The aim of this attack was for the fraudster to test when a transaction would be routed for 3DS authentication, thereby allowing the fraudster to make multiple fraudulent payments that fell just below the threshold and avoided the additional security measures required by Cdiscount's Payment Service Provider (PSP).

The ThreatMetrix solution helps Cdiscount detect this automated bot traffic by performing behavioral analysis of users during periods of normal operation and comparing such data to that gathered during an automate bot attack.

The Cdiscount Solution was Underpinned by the Following Core Capabilities from LexisNexis ThreatMetrix:

- **ThreatMetrix SmartID®:** 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, SmartID is based exclusively on device attributes to improve the detection of returning visitors, especially those trying to elude identification.

- **ThreatMetrix Mobile:** A lightweight software development kit (SDK) for Google Android and Apple iOS mobile devices, providing complete fraud protection for Cdiscount's mobile app. This includes advanced persistent device identification, anomaly and device spoofing detection, application integrity evaluation, malware detection, location services, jailbreak and root detection technologies.

- **TrueIP:** Reliably detects the use of location and identity cloaking services, such as hidden proxies and VPNs, allowing Cdiscount to see the true IP address, geolocation and other attributes of each transaction.

- **Champion Challenger:** Helps Cdiscount to determine the effectiveness of policy changes, as well as fine tune policies to keep pace with changes in consumer behavior and to stay ahead of emerging fraud patterns.

- **LexisNexis Risk Solutions Professional Services:** The Cdiscount professional services team provides hands-on fraud expertise, tailoring the LexisNexis ThreatMetrix solution to meet the unique and evolving requirements of Cdiscount. The team helps to continually optimize rules and policies to ensure that the full spectrum of fraud attacks are effectively detected, while minimizing false positives and manual reviews.

LexisNexis®
RISK SOLUTIONS

Learn more at 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 (LSE: REL/NYSE: RELX), a global provider of information-based analytics and decision tools for professional and business customers. For more information, please visit www.risk.lexisnexis.com and www.relx.com.

This document is for educational purposes only and does not guarantee the functionality or features of LexisNexis products identified. LexisNexis does not warrant this document is complete or error-free.