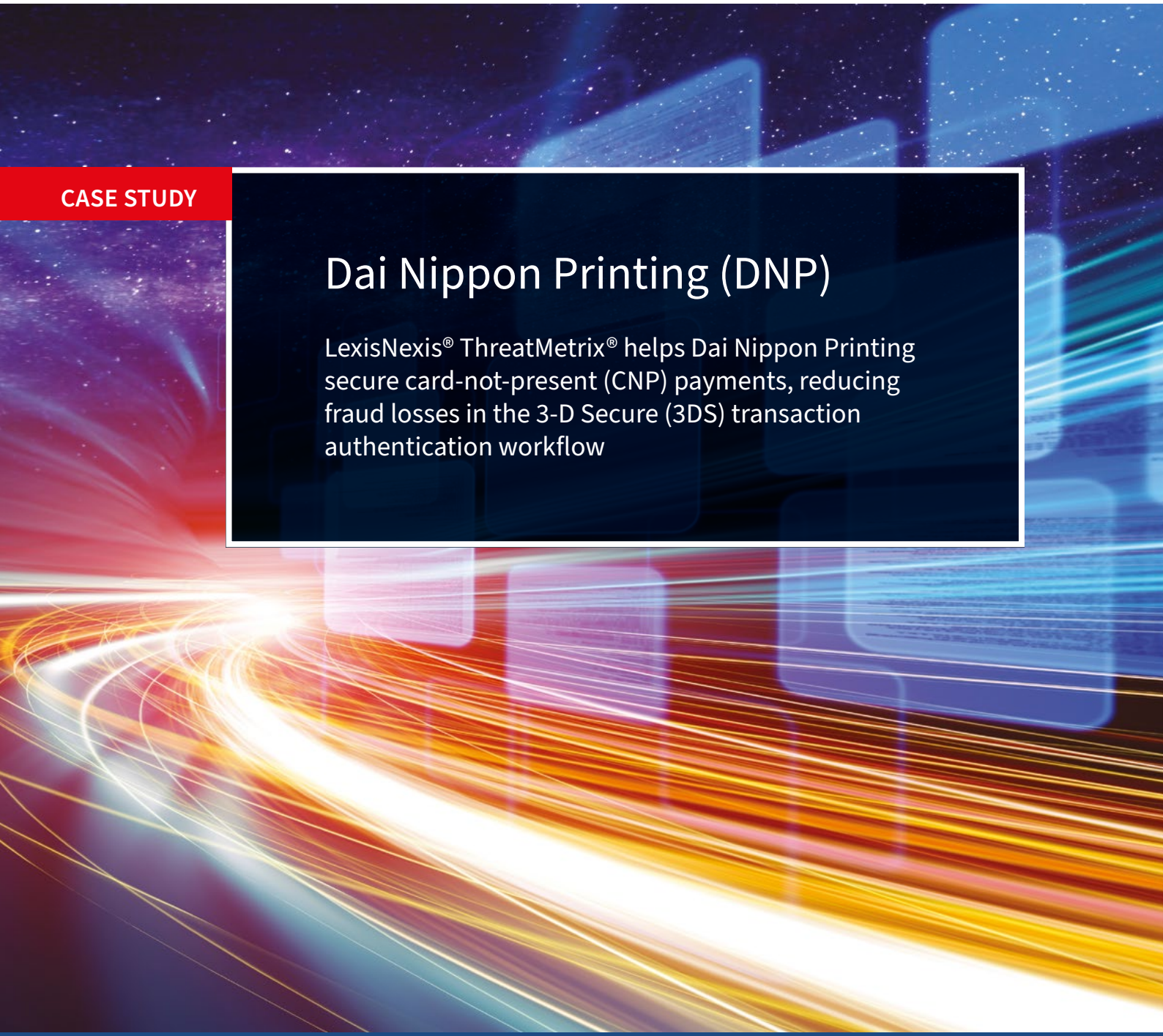
LexisNexis® RISK SOLUTIONS

Case Study: DNP



CASE STUDY

Dai Nippon Printing (DNP)

LexisNexis® ThreatMetrix® helps Dai Nippon Printing secure card-not-present (CNP) payments, reducing fraud losses in the 3-D Secure (3DS) transaction authentication workflow

"The ThreatMetrix solution helps us to accept more transactions and reduce cart abandonment because we are able to separate trusted behaviour from unusual behaviour, using our fraud resources to step-up genuinely high-risk payments." — DNP

Requirements

- Reduce card-not-present (CNP) fraud rates
- Reduce fraud losses for credit card issuers
- Provide an easily customisable, powerful rules engine
- Support DNP's competitive differentiation from other 3DS Access Control Server (ACS) provider

Solution

DNP uses risk-based authentication from LexisNexis® ThreatMetrix® to enhance risk decisioning as part of its 3DS workflow. Acting as the ACS provider for multiple Japanese card issuers, DNP can reliably identify high-risk transactions in near real time, helping card issuers decide whether to accept, reject or step-up CNP payment transactions. DNP provides a bespoke partnership with LexisNexis ThreatMetrix for those individual card issuers, allowing each organisation to implement risk-based authentication on their own payment workflows, with the ability to fine-tune rules and risk tolerance.

Bottom Line

- Low-risk transactions from trusted credit card customers can be authenticated with no associated friction, reducing unnecessary customer authentication and optimising the workload of the fraud department to focus on genuinely high-risk cases.
- A reliable risk assessment can be given for online payments, regardless of whether this is the first time the card has been used, or when a 3DS security password has not been registered.
- The LexisNexis ThreatMetrix solution enables card issuers to leverage global digital identity intelligence while tailoring transaction authentication strategies to their individual needs, via a partnership with DNP.
- Flexible, customised rules can be deployed to individual card issuers to reflect their individual business and fraud mitigation strategies.
- Issuers can share information relating to confirmed fraud using LexisNexis® Risk Solutions Consortium functionality.
- Fraud rates and fraud losses have been greatly reduced.

"The ThreatMetrix solution allows us to provide a best-in-class service to our issuers, helping to identify new and evolving fraud threats and respond with effective mitigation strategies." — DNP

Overview

DNP is a comprehensive printing company that was founded in 1876. By taking advantage of its P&I (printing and information) strengths, the company has expanded into a wide variety of business fields, including packaging materials, building materials and electronics. The company is also focusing on businesses that include the environment, energy and life science. DNP's Information Innovation Operations business unit focuses on digital marketing promotion as well as the expansion of cashless-settlement business. The unit also promotes BPO business that involves handling the operations of other companies, as one way to help address needs related to manpower shortages and work-style reforms. The unit boasted extensive domestic results in the marketing and settlement/authentication service businesses.

As part of DNP's settlement/authentication service businesses, the company provides a 3DS authentication solution, acting as the ACS provider for credit card issuers to authenticate CNP payment transactions using the 3DS protocol. During its dialogue with client companies, DNP identified the need to implement an effective risk-based authentication strategy to help issuers make more informed risk decisions and reduce fraud losses. This was particularly timely given the global escalation of CNP fraud.

With LexisNexis ThreatMetrix, DNP could:

- Look beyond credit card numbers and passwords, to passively risk-assess transactions by leveraging digital identity intelligence relating to devices, current and historic user behaviour, location data and transaction details.
- Separate trusted from high-risk transactions in near real time.
- Fine-tune rules and risk scores according to market requirements and evolving threats.

Business Problem

Electronic payments have revolutionised the way consumers transact, with cashless transactions now accounting for an ever-growing share of the Japanese market. However, with this change in consumer behaviour comes heightened risk, as fraudsters attempt to exploit the opportunities that digital payments present.

In its capacity as an ACS provider, card issuers were raising concerns to DNP that fraudsters were adopting ever-more sophisticated spoofing techniques to pose as legitimate consumers, often armed with a full array of stolen and spoofed credentials.

Issuers were faced with a growing fraud problem and escalating fraud losses. The key challenge was that standard identity verification and authentication checks could be easily passed by a fraudster in possession of a stolen identity and/or credit card credentials.

DNP needed a way to help issuers detect high-risk transactions, looking beyond static data and leveraging dynamic, near real-time digital identity data. DNP could alert issuers to, for example, a payment made using a stolen credit card, a device that had not previously been associated with a particular consumer, or suspicious transaction or location behaviour.

Enhancing 3DS risk decisioning using global digital identity intelligence

The LexisNexis ThreatMetrix solution is built on a crowdsourced repository of digital identity intelligence, harnessed from billions of global transactions across thousands of websites. The LexisNexis® Digital Identity Network® becomes more powerful with every transaction processed, giving organisations access to near real-time intelligence relating to consumers' digital identities.

This means that while a fraudster may have access to a stolen credit card, the Digital Identity Network can help issuers understand whether that credit card is being used by a new device, in a different location, with a different set of transaction behaviours, or from a device that is potentially compromised or infected with Malware.

Using hundreds of pieces of data to risk-assess every digital payment, DNP can therefore help issuers understand the trust or risk of a card-not-present transaction in near real time.

Extending the solution to allow tailored implementations for individual issuers, with sharing of confirmed fraud events via consortium

Following the success of the risk-based authentication approach for 3DS payments, DNP offered rule optimisation to individual issuers. This meant that issuers could implement tailored risk-based authentication approaches on their own online payment journeys, fine-tuning rules and risk scores to suit their particular fraud thresholds. DNP has currently onboarded more than 10 different Japanese issuers onto the LexisNexis ThreatMetrix platform, helping to build a fraud prevention solution that operates across the region.

To extend the success of these partnerships, these issuers have built a payments fraud consortium, using LexisNexis Risk Solutions Consortium functionality. This allows consortium members to share data related to confirmed fraud events with additional trust and context, within a defined group of organisations.

Benefits include:

- Tens of thousands of entities related to confirmed fraud events have been shared with organisations within the consortium.
- Several million Japanese yen are saved every month in prevented fraud, delivering a strong return on investment for consortium members.
- The ability to detect fraudulent transactions that cannot be completely protected by customer passwords alone.

"Consortium has been a game-changer for us—we are able to share what we are seeing with peers in our network, allowing us to collaborate and identify common fraud attributes and emerging attack vectors." — DNP

Specific features of the LexisNexis ThreatMetrix solution that help DNP reduce fraud losses from CNP transactions

- **ThreatMetrix SmartID®** enables DNP to identify 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 built on device specific attributes that improve the detection of returning visitors, especially those trying to elude identification.
- **Smart Rules** help DNP to better understand genuine customer behaviour, while reliably detecting genuine fraud. ThreatMetrix uses behaviour, age and location to examine the historical data related to a given transaction, in order to run a deep behavioural assessment. This helps DNP to more reliably differentiate between true fraud and legitimate behaviour change, reducing the step-up frequency without increasing overall risk.
- **LexisNexis ThreatMetrix Consortium** enables businesses with common goals, challenges or fraud risks to share their negative and positive data attributes in near real time, across an agreed set of consortium members and contributors. This knowledge sharing helps DNP detect and block fraudsters operating in networks across multiple organisations or testing stolen credentials across several online providers.
- **Champion Challenger** is used by DNP and several of the Japanese issuers to determine the effectiveness of policy changes without risk. A test policy (or Challenger) can be deployed in parallel without affecting the live policy (Champion). Both policies are executed simultaneously on the same events and can be compared for efficacy.

LexisNexis® RISK SOLUTIONS

To find out how we can help you and your business,
call 029 2067 8555 or email uk-irl-enquiry@lexisnexisrisk.com

risk.lexisnexis.co.uk/fraud-and-identity-management