

案例研究



# LexisNexis® ThreatMetrix® 帮助 大日本印刷实现安全的无卡支付， 减少 3-D Secure (3DS) 交易认 证工作流程中的欺诈损失

## 概览

### 客户

# DNP

大日本印刷 (DNP)

### 要求

- 降低无卡交易欺诈率
- 减少信用卡发卡机构的欺诈损失
- 提供一个易于定制、功能强大的规则引擎
- 提高 DNP 相比其他 3DS 访问控制服务器 (ACS) 提供商的差异化竞争优势

### 解决方案

DNP 利用 LexisNexis® ThreatMetrix® 提供的基于风险的身份认证以增强其 3DS 工作流程中的风险决策。作为日本多家发卡机构的 ACS 提供商，DNP 能够近实时地可靠识别高风险交易，帮助发卡机构决定接受、驳回还是进一步验证 CNP 支付交易。DNP 为各个发卡机构定制与 LexisNexis ThreatMetrix 的合作关系，允许各机构对其支付工作流程实施基于风险的身份认证，并对规则和 risk 承受能力进行微调。

### 概要

- 可信信用卡客户发起的低风险交易可以无摩擦进行认证，减少不必要的客户身份认证并优化防欺诈部门的工作量，使其能够专注真正高风险的案例。
- 不管是第一次用卡还是未注册 3DS 安全密码，都可以对在线支付进行可靠的风险评估。
- LexisNexis ThreatMetrix 解决方案使发卡机构能够利用全球数字身份情报，通过与 DNP 合作根据自身需求定制交易认证策略。
- 为各个发卡机构部署灵活的、量身定制的规则，体现出其各自的业务及欺诈缓解策略。
- 发卡机构可以利用 LexisNexis® Risk Solutions 的 Consortium 功能共享与已确认的欺诈相关的信息。
- 欺诈率和欺诈损失大大降低。

“有了ThreatMetrix解决方案，我们能够为发卡机构提供一流的服务，帮助识别不断变化的新欺诈威胁并采取有效的缓解策略。” — DNP

### 总览

DNP 是一家综合性印刷公司，成立于 1876 年。凭借其 P&I（印刷和信息）优势，公司已扩张至多个业务领域，包括包装材料、建筑材料和电子产品。公司同时还致力于环境、能源和生命科学等业务。DNP 的信息创新运营业务部门专门从事数字营销推广以及无现金结算业务拓展。该部门还推广涉及其他公司业务经营的 BPO 业务，帮助解决与劳动力短缺和工作方式变革相关的需求。该部门在国内营销和结算 / 认证服务业务方面取得了广泛的成果。

作为 DNP 结算 / 认证服务业务的一部分，公司提供了一款 3DS 身份认证方案，以信用卡发卡机构 ACS 提供商的身份用 3DS 协议对 CNP 支付交易进行身份认证。DNP 在其与客户公司的对话过程中发现了实施有效的、基于风险的身份认证策略，以帮助发卡机构做出更合理的风​​险决策、降低欺诈损失的需求。鉴于 CNP 欺诈的全球升级，这一发现尤为及时。

有了LexisNexis ThreatMetrix之后，DNP可以：

- 在信用卡卡号和密码之外，通过利用与设备、当前和历史用户行为、位置数据和交易细节相关的数字身份情报，被动地评估交易风险。
- 近实时区分可信交易与高风险交易。
- 根据市场需求和不断变化的威胁微调规则和风险分值。



### 业务问题

电子支付彻底改变了消费者的交易方式，无现金交易在日本市场的份额越来越大。但是，随着消费者行为的这种变化，风险也随之增加，因为欺诈者试图利用数字支付获取收益。

作为一个 ACS 提供商，DNP 了解到发卡机构对欺诈者采用越来越复杂的欺骗技术冒充合法消费者（通常利用各种被盗和伪造的凭证）这一现象表示的担忧。

发卡机构面临着日益严重的欺诈问题以及越来越多的欺诈损失。

关键问题是，拥有被盗身份和 / 或信用卡凭证的欺诈者很容易通过常规的身份验证和认证检查。

DNP 需要在静态数据以外，利用动态且近实时的数字身份数据来帮助发卡机构检测高风险交易。例如，DNP 可以向发卡机构提示用被盗信用卡做出的支付、未曾与特定消费者关联的设备、可疑的交易或位置行为。

**“ThreatMetrix 解决方案可以帮助我们接受更多交易、减少弃单，因为我们能够区分可信行为和异常行为，利用欺诈信息资源进一步审核真正高风险的支付。” — DNP**

### 利用全球数字身份情报加强 3DS 风险决策

LexisNexis ThreatMetrix 解决方案建立在一个由数千个网站上数十亿笔全球交易形成的众包数字身份情报库基础上。每处理一笔交易，LexisNexis® Digital Identity Network® 就随之更加强大，让企业能够获得与消费者数字身份相关的近实时情报。

这意味着，虽然欺诈者可能获得被盗信用卡，Digital Identity Network 则可以帮助发卡机构了解该信用卡是否在新设备、不同位置上以不同的交易行为使用，或者是否在可能受到恶意软件危害或感染的设备上使用。

因此，利用数百条数据对每笔数字支付进行风险评估，DNP 可以帮助发卡机构近实时地了解无卡交易的可信度或风险。

### 扩展解决方案，使各发卡机构可以通过联盟共享已确认的欺诈事件，并定制其自身配置

基于风险的身份认证法在 3DS 支付领域获得成功后，DNP 为各个发卡机构进行了规则优化。这意味着发卡机构可以对其在线支付过程实施基于风险的定制身份认证，对规则与风险评分进行微调以适应其具体的欺诈阈值。DNP 目前已将日本 10 多家不同的发卡机构纳入 LexisNexis ThreatMetrix 平台，帮助建立一个覆盖整个地区的欺诈预防解决方案。

“我们与日本市场许多发卡机构都有往来——所有这些机构都面临不同的欺诈难题和攻击模式。有了 ThreatMetrix，我们可以为各发卡机构提供定制解决方案，这是我们在选择 LexisNexis Risk Solutions 时的一大优势。” — DNP

发卡机构利用 LexisNexis Risk Solutions 的 Consortium 功能，建立了一个防支付欺诈联盟，来进一步推动彼此合作的成功。联盟成员可以在这个环境下更放心在固定的企业团体内共享与已确认欺诈事件相关的数据。

#### 优势包括：

- 已与联盟内的企业共享了与已确认欺诈事件相关的数万个实体。
- 所预防的欺诈每月节省了数百万日元，为联盟成员带来丰厚的投资回报。
- 能够检测单靠客户密码无法完全保护的欺诈性交易。

“联盟对我们来说是一个游戏规则的改变者——我们能够与我们网络中的同行分享我们所看到的，从而实现合作并发现常见的欺诈属性和新兴的攻击途径。” — DNP

## LexisNexis ThreatMetrix解决方案中帮助DNP减少CNP交易欺诈损失的具体特征

- **ThreatMetrix SmartID®** 让 DNP 可以识别消除 Cookie 信息、使用无痕浏览以及篡改其他参数以绕过设备指纹识别的现有用户。此项功能可以帮助检测现有用户，降低误报。SmartID 源于对众多浏览器、插件和 TCP/IP 连接属性进行的分析，它建立在设备特定的属性上，可以加强对回访者的检测，尤其是尝试规避识别的回访者。
- **Smart Rules** 能够让 DNP 更好地理解真实客户行为，同时更可靠地检测真实的欺诈行为。ThreatMetrix 用行为、年龄和位置信息审查给定交易有关的历史数据，进行深层的行为评估。从而帮助 DNP 更加可靠地区分真实欺诈与合法行为变化，减少进一步审核的频率同时却不增加整体风险。
- **LexisNexis ThreatMetrix Consortium** 让具有共同目标、面临共同挑战或欺诈风险的企业能够在一批达成协议的联盟成员和参与者之间近实时地共享其负面和正面数据属性。此种知识共享能够帮助 DNP 检测并阻止欺诈者在跨机构的网络中活动，或针对多个在线提供商测试被盗凭证。
- DNP 和多个日本发卡机构均采用 **Champion Challenger** 来判定策略改变在不造成风险情况下的有效性。可同时部署一个测试策略（或 Challenger）而不影响现有策略（Champion）。对相同事件同时实施两种策略，并对其效力进行对比。

更多信息，请登录[risk.lexisnexis.com/FIM-ZH](http://risk.lexisnexis.com/FIM-ZH)



### 关于LexisNexis Risk Solutions

LexisNexis® Risk Solutions 利用数据和高级分析技术提供深刻见解，帮助企业和政府机构降低风险和改善决策，从而造福全球人民。公司为保险、金融服务、医疗保健和政府等广泛行业提供数据和技术解决方案。公司总部设在美国乔治亚州亚特兰大市，并在全球各地都设有办事处。本公司是 RELX 集团（LSE: REL/NYSE: RELX）旗下的一个业务部门，后者为全球专业和商业客户提供基于信息的分析技术和决策工具。

欲了解更多信息，请访问：[www.risk.lexisnexis.com](http://www.risk.lexisnexis.com) 和 [www.relx.com](http://www.relx.com)。

### 关于ThreatMetrix

ThreatMetrix® 是 LexisNexis® Risk Solutions 旗下公司，它能够增强全球经济实现盈利和安全增长的能力而不损害其安全性。凭借其对于 14 亿个标记化数字身份的深入了解，LexID® Digital 提供了 1.1 亿个日常身份验证和信任决策相关的情报，以近实时区分合法客户和诈骗者。ThreatMetrix 和 Digital Identity Network 是 ThreatMetrix, Inc. 的注册商标。

本文件仅供指导，不保证所述 LexisNexis 产品的功能或特性。LexisNexis 不保证本文件的完整性与准确性。

LexisNexis 和 Knowledge Burst 标识是 RELX Inc. 的注册商标。ThreatMetrix、Digital Identity Network 和 ThreatMetrix SmartID 是 ThreatMetrix, Inc. 的注册商标。© 2021 LexisNexis Risk Solutions 版权所有。NXR14802-01-0221-CH-S