LexisNexis®
RISK SOLUTIONS

CASE STUDY

LexisNexis® Risk Solutions works in partnership with UK Bank to ensure that catching criminals does not compete with customer experience

UK bank uses LexisNexis® ThreatMetrix® intelligence to increase good customer recognition, better detect genuine fraud and achieve compliance with PSD2 Strong Customer Authentication (SCA).

AT A GLANCE

CUSTOMER

Tier 1 UK Bank

REQUIREMENTS

- Deliver a low-friction online experience for good, trusted customers.
- Provide tailored online journeys for different customer risk profiles.
- Stop fraud losses.
- Achieve compliance with PSD2 regulations to optimise cost and customer management.

SOLUTION

Using the LexisNexis® Digital Identity Network® and ThreatMetrix® product capabilities, this tier 1 UK bank can better understand the trustworthiness of its customers from the moment they apply for a new product or service, and throughout their lifecycle; at login, change of details and payments. This is underpinned by several key capabilities including: advanced online risk assessments, silent authentication strategies, customer-focused analytics, machine learning, and consortium functionality that shares intelligence across the organisation and the UK banking network.

BENEFITS

- A holistic view of trust and risk across the customer lifecycle.
- Protect new account/product applications by identifying high-risk individuals and customers at risk in near real-time.
- Fewer customer interventions and associated step up costs using silent risk assessment on web and mobile login.
- Significant reduction in false positives, so good customers experience less friction.
- Optimised fraud detection using flexible rules that differentiate between unusual customer behaviour and genuine high-risk events.
- Prevent mule-related money transfers by detecting mule accounts through analysing links between devices and accounts.
- Leveraging Consortium capability to share intelligence related to known fraud and mule devices.
- Achieve PSD2 compliance using Strong ID device binding online for silent, persistent and strong authentication.

CASE STUDY

“By reducing false positives, we have been able to reinvest the alerts and the headcount back into refining our strategy, stopping fewer people but more fraud.”

— TIER 1 UK BANK

Overview

As a leading provider of financial services, this UK bank has millions of customers, both personal and commercial.

A key strategic priority is to provide simpler, streamlined customer interactions on web and mobile. Yet while customers expect low-friction account access, the bank continually faces having to introduce more interventions due to an evolving regulatory landscape and ever-more sophisticated cyberattacks.

The bank required a solution that provides persistent device recognition and digital identity intelligence to better understand the legitimacy of digital interactions, with the ability to identify the full spectrum of fraudulent behaviour in near real-time, without affecting good customers.

“Detecting and blocking mule accounts is the apex of the fraud triangle; if you catch the mules, you reduce virtually all banking fraud. Our partnership with LexisNexis® Risk Solutions has been a true collaboration to genuinely understand the anatomy of mule behaviour; to mitigate it both now and in the future.”

—TIER 1 UK BANK

Business Problem

The bank, as with all global financial institutions, walks a tightrope between effective fraud control and exceptional customer experience. The balancing act is precarious and has to tackle global networks of criminal behaviour as well as fraudsters targeting individual customer accounts:

- Organised and hyper-connected mule networks continue to infect the banking system, filtering proceeds of crime across country borders, facilitated by faster payments.
- Fraudsters target customers as the weakest link in the security chain with pitch-perfect social engineering attacks that often piggy-back fully authenticated online banking sessions via remote access tools, making them very hard to detect.
- Regulations such as PSD2 seek to promote competition, innovation and heightened security. Yet customers don't tolerate interventions they consider to be unnecessary.

"Customer behaviour is also becoming more diverse and less predictable than ever before" said the UK bank. *"Definitions of 'normal' are becoming somewhat redundant. Our fraud systems have to be able to model a rich array of legitimate customer behaviour without catching good customers in the net".*

A flexible approach to understanding customer identities powered by digital identity intelligence

ThreatMetrix Digital Identity Intelligence unites information related to devices, locations, behaviours and threats to help the bank connect the dots between the myriad pieces of information a customer creates as they transact online, looking at relationships between entities at a global level and across channels/touchpoints. Specific ThreatMetrix product capabilities utilised by the bank include:

Smart Rules

Smart Rules analyse behaviour on an individual customer level, comparing current event data to what is normal for that customer. This approach isolates genuinely high-risk transactions from those that may seem unusual, but form part of a customer's normal online footprint. Using Smart Rules, the bank can configure dynamic thresholds, calculated based on the context of the transaction, e.g. to compare current events with historical information specific to the customer.

> *"What Smart Rules have enabled us to do is to tailor rules and strategies for individual behavior rather than assuming that everyone behaves in the same way, which of course is not the case. We can better differentiate between true fraud, and legitimate "strange" behaviour."*

—TIER 1 UK BANK

ThreatMetrix Portal

The Portal allows the bank to create offline models using Th eatMetrix data which are then introduced into the bank's policy using the inline variable rule. These fraud models enable the bank to better identify risk, create cases and allow operational teams to review and investigate alerts.

> *"The ThreatMetrix Portal, in terms of case reviews, recalls and the flexibility of rules, is excellent. This is one of the key strengths for LexisNexis® Risk Solutions relative to its competitors."*

—TIER 1 UK BANK

ThreatMetrix Mobile SDK

ThreatMetrix Mobile is a lightweight soft are development kit (SDK) for Google Android and Apple iOS mobile devices, supporting complete authentication and fraud protection for the mobile channel.

Anomaly and device spoofing detection help the bank detect device emulation, tampering, root/jailbreak cloaking, and other anomalies that may indicate fraud.

Strong ID

ThreatMetrix Strong ID is one of three device fingerprinting capabilities within the ThreatMetrix product. Strong ID creates a cryptographic bind between a customer’s web/mobile browser/app and ThreatMetrix for persistent and secure device recognition, meeting SCA possession-based compliance for PSD2.

The bank is currently using Strong ID for web, to optimise the strategies for additional authentication solutions, thereby reducing unnecessary interventions and costs associated with step-ups and step-up failure.

Consortium

Consortium creates an industry-focused layer that compliments an organisation's local intelligence and the global shared intelligence harnessed through the LexisNexis® Digital Identity Network®. The information can be operationalised by configuring strategies on the data shared at the consortium level within ThreatMetrix policies.

The bank is currently part of a UK banking Consortium, benefitting from sharing information across different use cases. Benefits include:

- Sharing of historic blacklisted devices
- Proactive identification of mule accounts, and associated fraud strategies
- Near real-time sharing of bad attribute data
- More accurate tracking of high-risk devices: banks can access additional context behind risk decisions such as when an entity was blacklisted and by which other bank(s)

LexisNexis®
RISK SOLUTIONS

For more information, call 029 2067 8555
or email uk-irl-enquiry@lexisnexisrisk.com

risk.lexisnexis.co.uk

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 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 across industries. For more information, please visit risk.lexisnexis.co.uk and www.relx.com.

This document is for informational purposes only and does not guarantee the functionality or features of any LexisNexis Risk Solutions products identified.
LexisNexis Risk Solutions does not represent nor warrant that this document is complete or error free.