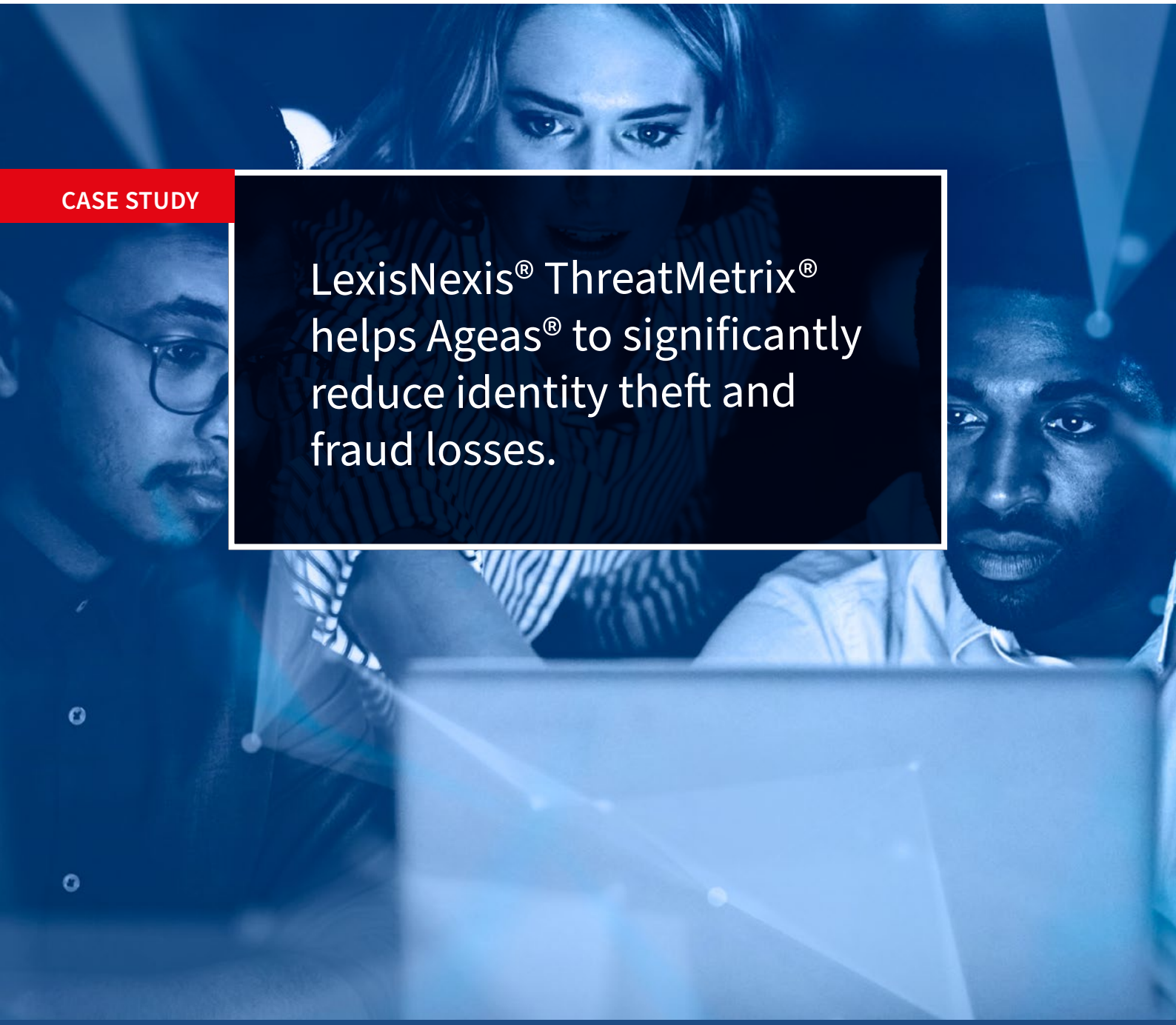
LexisNexis®
RISK SOLUTIONS

ageas



CASE STUDY

LexisNexis® ThreatMetrix® helps Ageas® to significantly reduce identity theft and fraud losses.

Ageas, one of the leading insurers in the UK, gains a clearer perspective on identity authentication and fraud prevention with LexisNexis® Risk Solutions.

Customer

Ageas® – Motor and Home Insurance

Business Challenge

As one of the largest home and motor insurers in the UK, Ageas was looking to significantly drive down the cost of fraud and improve its ability to authenticate the identity of prospective and existing customers. Despite having a range of existing fraud prevention and IDV tools already in place they still believed that it was possible to enhance these capabilities, and drive significant ROI and cost reductions through the use of additional intelligence.

Specific Requirements

- Prevent identity theft
- Significantly reduce fraud losses
- Enhance anomaly intelligence for hard to find fraud typologies
- Provide fresh intelligence to more comprehensively assess risk
- Easily integrate with existing technology workflows

The Solution

Ageas used intelligence from LexisNexis® ThreatMetrix® to improve its ability to protect its customers identities and further minimise the risk of fraudulent policy applications being accepted. The ThreatMetrix® solution combined a unique layer of intelligence attributes that Ageas previously did not have access to. Adding device, location and various other behavioural biometric insight for example into their intelligence universe. This gave Ageas a much clearer perspective on a potential customer's level of risk and true identity. This capability also enabled them to detect anomalies or suspicious behaviours faster, and more cost effectively, to support a more accurate and timely decision making process.

Business Problem In Detail

Identity theft and application fraud are huge and growing problem for the Insurance industry. The latest figures from CIFAS shows that there was an 11% rise in identity theft in 2021 with the FCA projecting the cost of this at over £78 Million to the UK. Additionally the amount of insurance fraud in the UK is estimated by the ABI to be costing around £1.3 Billion with average fraudulent claims now costing £12,000 per claim.

As a reputable insurer, Ageas wanted to be confident it was doing everything it could to protect its customers and the organisation from these issues. The company was concerned it was not always detecting fraud until too late in the process and wanted to be better equipped to improve its ability to speed up the resolution of fraud investigations as well as uncovering identity theft.

The company was interested in a solution that combined the latest threat intelligence (on known fraudsters and compromised devices or credentials), with sophisticated software and analytics capable of detecting anomalies and suspicious behaviour upfront. Ageas were also interested in gaining access to a much wider level of intelligence that it did not have visibility of, for example unexpected connections between people making applications; multiple applications from the same device; applications from unexpected locations; or the use of newly created email addresses, that might indicate a higher risk of fraud and therefore require further investigation before the application is accepted.

It takes a Network to Fight a Network

Using LexisNexis® ThreatMetrix®, and in particular its device identification capabilities such as ExactID and SmartID, Ageas has significantly improved its ability to identify fraudulent links and associations that would otherwise have gone unnoticed.

Ageas now layers together a range of additional identity attributes such as device ID, GPS location data, email addresses and behavioural biometrics, to help identify fraud risk far more effectively, at the point of application.

LexisNexis ThreatMetrix draws on shared, global intelligence from millions of daily consumer interactions, including logins, payments and new account applications, which are collected and processed through the LexisNexis® Digital Identity Network®. Using this information, the ThreatMetrix solution creates a unique digital identity for each and every user, based on an analysis of the myriad of connections that users make as they transact online. In this way the digital identity profile helps organisations to recognise trusted users and what is normal for them, and highlights anomalies.

SmartID Helps Ageas Identify First Ghost Broking Fraud Ring

During the initial testing phase, one particular policy was reviewed to ensure the API was working as expected. The 'Related Events' feature was employed, which successfully identified an additional three policies linked to the first. On further investigation it became clear that all three policies had been set up in the same month. The SmartID® capability was then able to link all four policy applications back to the same device.

Ageas reviewed each of the four policies within their own policy admin system and saw that there had been no concerns flagged. One of the policies even had a record of the applicant having supplied proof of a No Claims Discount. However, further investigations resulted in all four policies being cancelled for ghost broking – the No Claims Discount turned out to be a doctored document.

Without the ThreatMetrix solution, Ageas would not have identified the link between the policies and the fraud ring would not have been identified..

"Ageas has taken a mature approach to data by ensuring cross-functional alignment is part of our core ethos. Whereas fraud is often considered under the spotlight of claims, ThreatMetrix enables us to identify fraud from the perspective of policy inception. Its algorithms and ruleset opens up a whole new layer of fraud protection."

– **Adam Clarke**, Chief Underwriting Officer, Ageas UK

Ageas leverages several capabilities from the ThreatMetrix solution, including:

- **LexID® Digital** brings together online and offline data attributes for each transacting user, including device-related intelligence, tokenised email/physical addresses, telephone numbers and credit card hashes. Through the analysis of billions of online transactions, it identifies complex associations between events and allows Ageas to recognise a person's true identity, irrespective of changes in devices, locations or behaviour.
- **ThreatMetrix SmartID®** identifies returning users even when they choose to wipe cookies, use private browsing, and change other parameters, to bypass device fingerprinting. Derived from the analysis ofmany different browsers, plug-ins, and TCP/IP connection attributes, SmartID improves returning user detection and reduces false positives.
- **ThreatMetrix deep connection technologies** give Ageas a clearer view of anomalous or suspicious events. Fraudsters often attempt to hide behind location and identity cloaking services such as hidden proxies, VPNs and TOR browsers. The ThreatMetrix solution reliably detects the use of these technologies and, in the case of proxies and VPNs, allows Ageas to see the true IP address, geo-location and other attributes relating to each event, supported by global identity data, over time.
- **Trust Tags** enable Ageas to differentiate between fraudsters and legitimate users by dynamically associating any combination of online attributes involved in accepting, rejecting or reviewing a transaction. Trust Tags act as digital labels that can be applied to various combinations of attributes within a user's persona to indicate their trustworthiness, reducing friction for legitimate users and more reliably identifying high-risk behaviour.

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