LexisNexis® RISK SOLUTIONS

Case Study:

One Call INSURANCE

CASE STUDY

One Call Insurance

One Call Insurance Switches to LexisNexis® Risk Solutions and Increases Fraud Detection Rate by ~60%.

One Call Insurance is Cemented as One of the Top Anti-Fraud Insurance Brokers in the UK.

"The massive benefit we saw from ThreatMetrix is that it is giving us transparency of a fraudulent policy or fraud ring from the outset." – Josh Barnsdale, One Call Insurance

Requirements

- Reduce fraudulent new policy applications.
- Reliably detect ghost brokers and organised fraud rings.
- Streamline the fraud review process.
- Reduce fraud losses.

Solution

By switching to LexisNexis® ThreatMetrix®, One Call Insurance was able to leverage global shared intelligence relating to an applicant's true digital identity.

Bottom Line

- The ThreatMetrix solution has increased the fraud detection rate by approximately 60 percent compared to the incumbent device-based fraud solution.
- One Call Insurance has earned the reputation as one of the top anti-fraud brokers in the UK.
- A more proactive, streamlined approach to detecting high-risk cases.
- Reduced exposure to third-party liability on fraudulent policies, as well as reduction in fraud losses from false claims.

Overview

One Call Insurance is one of the largest independent insurance brokers in the UK. Founded in 1995, One Call Insurance hit the 500,000 customer milestone in 2018, writing millions in gross written premiums. It was experiencing a wide range of fraud, including:

- Ghost brokers and organised fraud rings trying to obtain fraudulent policies.
- Individuals switching from different insurance companies after defaulting on payment.

When One Call Insurance switched to LexisNexis ThreatMetrix, it was able to:

- Analyse every new policy application in the context of the applicant's digital identity, identifying any anomalies or high-risk behaviour that could indicate fraud.
- Reject applications that looked fraudulent before providing coverage.

Business Problem

Despite a robust fraud detection solution, One Call Insurance couldn't always identify a fraud ring or ghost broker until it saw subsequent policies with unusual links to the first. The initial policy slipped under the radar, then another policy appeared from the same device, or with the same email address or telephone number, and the fraud ring was exposed. It was missing the opportunity for early, proactive detection.

One Call Insurance needed a solution that could authenticate all applications from the outset, looking holistically at connections between devices, locations, email addresses and threat intelligence to detect anomalies that might indicate fraud right from the first application.

"The system is a lot easier and it has sped up the process. We are now much more confident—when there is no flag by ThreatMetrix, there is a minimal chance of fraud." — Josh Barnsdale, One Call Insurance

Leveraging ThreatMetrix Digital Identity Graphs to reliably identify fraud rings

The ThreatMetrix solution is underpinned by the LexisNexis® Digital Identity Network® which harnesses global shared intelligence from millions of daily consumer interactions including logins, payments and new account applications. Using this information, the ThreatMetrix solution creates a unique digital identity for each user by analysing the myriad connections between devices, locations and anonymised personal information.

Digital Identities are created by combining the following key intelligence:

- **Device Profiling** – Device identification, device health and application integrity, as well as detection of location cloaking or spoofing, (proxies, VPNs and the TOR browser).
- **Threat Intelligence** – Harnessing point-in-time detection of malware, Remote Access Trojans (RATs), automated bot attacks, session hijacking and phished accounts, then combining with global threat information such as known fraudsters and botnet participation.
- **Identity Data** – Incorporating tokenised, non-regulated personal information such as user name, email address, telephone number and more.
- **Behaviour Analytics** – Defining a pattern of trusted user behaviour by combining identity and transactional metadata with device identifiers, connection and location characteristics. Every transaction can be analysed in the context of this behaviour pattern and historic context globally.

One Call Insurance could authenticate every new policy request against this trusted and unique online digital identity, checking whether credentials of the applicant correlated with anonymised information held by the Digital Identity Network.

Long-term success

- **One Call Insurance** took advantage of the flexibility of the ThreatMetrix policy engine to customise risk scores to suit its specific business requirements.
- **ThreatMetrix Trust Tags** enabled One Call Insurance to effectively differentiate between fraudsters and legitimate applicants. Trust can be associated dynamically with any combination of online attributes such as devices, email addresses, card numbers or any other attributes involved in accepting, rejecting or reviewing an insurance application. This capability had a big impact on streamlining the policy approval processes.
- **Following successful deployment**, One Call Insurance is looking at extending the solution to help prevent fraudulent claims.

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