iovation
A TransUnion® Company

THE ESURE INSURANCE CASE STUDY

ESURE CUTS CALL CENTER FRAUD BY 40% WITH IOVATION

CHALLENGES

Fraudsters had learned that they couldn't beat iovation on esure.com. So, the criminals launched an omnichannel attack. Between the use of stolen PII and the absence of device recognition, fraudsters' applications were more likely to be approved through the call center.

SOLUTIONS

esure changed its e-fulfillment policy. Instead of emailing new customers their documents, esure would send a link to a customer portal. Once again, fraudsters couldn't get past iovation at the new portal's registration and login pages.

RESULTS

Every time fraudsters use a new tactic, esure responds by modifying its implementation of iovation for real-time feedback and impact. esure plans to implement iovation's omnichannel solution at its electronic notification of claims soon.

esure

OMNICHANNEL FRAUD DETECTION AND PREVENTION STRATEGY EMERGES FROM FIVE-YEAR SUCCESS FIGHTING GHOST BROKING RINGS WITH DEVICE RECOGNITION

I'D INTENDED TO RUN A 75-DAY PROOF OF CONCEPT BEFORE MAKING A DECISION. WITHIN THE FIRST FORTNIGHT IT WAS EVIDENT IOVATION HAD DOUBLED OUR FRAUD DETECTION. WE DISCOVERED ENOUGH ORGANISED FRAUD TO COME TO THE CONCLUSION WE NEEDED TO KEEP IT SWITCHED ON.

Matt Gilham, Head of Financial Crime, esure

"We were stopping their devices online, so they began coming through our call center. They knew we couldn't track them when they called in. Once we figured that out, we made a small change to our e-fulfillment process that cut our fraud rate by 30-40%."

Meet Matt Gilham, Head of Financial Crime at esure, one of the UK's leading providers of motor and home insurance products.

Just like other UK insurers today, esure gets the majority of its new policy applications through insurance aggregation websites.

The rise of digital applications for insurance policies brought with it an increasing number of bad policies. That led Gilham to add device recognition to his fraud-fighting stack in late 2013.

"Originally, the intention was to run a 75-day proof of concept with iovation, but within the first fortnight we had doubled our fraud detection," Gilham recalls. "Although we were in the middle of our budget cycle, I approached my executives saying 'we can't switch this off, please can I have some additional budget?''

Increase the cost to commit fraud

Since that proof of concept, esure has continuously raised their guard against fraudsters without impacting the experience for its legitimate customers. The opportunists have gone elsewhere, but the better-organised and -funded rings have increased the sophistication of their tactics.

When esure added real-time blocking of devices applying for motor insurance on their site, the fraudsters turned to the aggregators to solicit quotes and submit applications.

Then, esure and a leading market aggregator teamed up in 2015 to create business rules that stopped bad devices from viewing esure's policy quotes on the aggregator's site.

esure enjoyed a lull in its fraud rate for months after each change. But the fraudsters would not go away.

BEFORE WE STARTED BLOCKING BAD DEVICES IN REAL TIME WITH IOVATION, 70% OF OUR BAD POLICIES WERE INCEPTED FROM ONLINE SOURCES. THE REST CAME OVER THE TELEPHONE. THAT RATIO REVERSED AFTER WE'D STARTED REAL-TIME BLOCKING ON OUR SITE, AND BEGUN COLLABORATING WITH A LEADING MARKET AGGREGATOR.

Matt Gilham, Head of Financial Crime, esure

Over the phone, synthetic identities would be denied by esure's identity and financial stress scoring services, but the stolen Personal Data of a reputable victim would slip through. As soon as the call center agent incepted the policy, the fraudster would receive an automatic email with a link to download the policy documents.

Then, it was just a matter of time before a bad claim or a distraught ghost-broking victim would follow.

"When we began to investigate, I remember one case in particular where we saw the same device downloading 50, 60, 70 different policies," Gilham marvels. "All in different people's names, all after having transacted through the call center."

ID checks pass. Device checks deny.

While the fraudsters could change the ways they applied for esure's policies, and use stolen PII to pass identity checks, they were still reliant on an Internet-connected device to conduct their business. That single point in the process remains fraudsters' weakness; thanks to iovation.

iovation's device recognition technology uses thousands of permutations of device attributes to identify a device instantly and continue to recognise it over time. (Coincidentally, this feature complements the GDPR's mandates for data minimisation and privacy by design.).

When any of iovation's 4,000-plus Community of users encounters fraud from a device visiting their site, they place specific evidence of fraud against the device in iovation's database of over 5 billion devices, the world's richest.

Every anti-fraud professional involved is intrinsically motivated to add the highest quality of evidence to iovation's 55 million reports of fraud and abuse.

AFTER IMPLEMENTING IOVATION'S REAL-TIME BLOCKING, WE REDUCED THE VOLUME OF FRAUD ATTACKING US BY 70%.

Matt Gilham, Head of Financial Crime, esure

"The evidence from iovation's Intelligence Center helps my investigators to confirm their suspicions about the devices associated with dubious policies or claims," says Gilham.

With more than 40 evidence types to choose from – ranging from reports placed against a device to technical anomalies like Tor nodes and proxy servers – Gilham and his team can create endless combinations of compound rules to sharpen their transaction decisioning process. Rules can be tuned in real time for immediate and precise control over how each visiting device will be treated.

"Back in 2013 iovation was the standout option," Gilham explains. "That hasn't changed. The unique device ID allows us to identify and monitor suspect devices and accounts with exquisite precision. We get more value out of iovation's Intelligence Center with every insurer that joins. Most critically, we can quickly adapt our implementation of iovation as fraudsters shift their tactics."

Closing loophole cuts fraud rate by more than 40%

After discovering the 'call center loophole' that fraudsters were exploiting, esure created a portal for customers' documents. This was a convenient, secure place for honest customers to access and store their documents in the cloud. For fraudsters, it was the end of the line. If they tried to register an account or log in with a hot device, iovation's business rules stopped them cold.

"Since we began blocking bad devices at the portal, our fraud rate has decreased by a solid 40%. It's somewhat counterintuitive, but we've seen a drastic reduction of telephony fraud due to having iovation on the web," says Gilham. That decline brings a cascade of benefits to esure; "We get more value from our acquisition and onboarding efforts. Our manual review process is more productive. And we have fewer suspect claims to investigate."

ABOUT IOVATION

iovation, a TransUnion company, was founded with a simple guiding mission: to make the Internet a safer place for people to conduct business. Since 2004, the company has been delivering against that goal, helping brands protect and engage their customers, and keeping them secure in the complex digital world. Armed with the world's largest and most precise database of reputation insights and cryptographically secure multi-factor authentication methods, iovation safeguards tens of millions of digital transactions each day.

iovation.com

Global Headquarters

iovation, a TransUnion company
555 SW Oak Street, Suite #300
Portland, OR 97204 USA

PH +1 (503) 224 - 6010
FX +1 (503) 224 - 1581
EMAIL info@iovation.com

United Kingdom

PH +44 (0) 800 058 8731
EMAIL uk@iovation.com

iovation®
A TransUnion® Company