BAE SYSTEMS
INSPIRED WORK

Insurance Fraud: The value of integrating third-party data

Interview with Dan Gumpright

Just like any other sector, new customers are costly for insurers to come by. It's now also much easier for customers to switch suppliers so retention has also become more difficult. Many Insurers are focussing on customer experience improvements to address this problem and particularly on how detecting fraud impacts genuine customers.

Insurance Product Manager Dan Gumpright at BAE Systems, discusses the role third-party data can play in enhanced fraud targeting, and how this is helps insurers tackle this issue.

Q: What is driving the need for Insurers to consider further data integration – are systems simply not good enough, or are fraudsters getting cleverer?

A: Globally, insurance fraud is the second largest and most financially lucrative criminal enterprise after illegal narcotics. For that reason, whenever Insurers put fraud defences in place to stop the progression of organised crime, fraudsters will either retaliate, or find a way around. Criminals are continually and rapidly evolving and the speed at which they develop new behaviour is impressive. In order to keep up, Insurers need to maintain technical agility.

Q: What is the link between fraud and customer service?

A: Many insurance executive teams that I talk to are taking a zero-tolerance approach to how fraud impacts genuine customers. The challenge of both validating genuine customers and spotting fraudsters, requires Insurers to move faster than before. Claims have to be resolved quicker and customers are increasingly expecting faster claim resolution and payment. In many markets this is also driven by regulation. A certain percentage of claims normally have to be resolved within 24 hours, or five working days. The challenge Insurers face is they know that somewhere between 10 and 20 per cent of claims contain fraud – either opportunistic or criminally organised. But how do you find that one-in-five, and at the same time not slow down payment to your genuine customers?

Q. Is the use of third-party data the solution?

A: Insurers hold a large amount of data that can be harnessed for effective fraud detection. The growth of Artificial Intelligence, Internet of Things and smart devices is rapidly increasing the amount of data Insurers have access to. The challenge is knowing how to apply that wealth of data alongside past customer behaviour to specific areas such as how claims fraud detection aides in streamlining the claim resolution process and payment, increases profitability and enhances customer satisfaction.

Over and above the information an individual Insurer has access to, there is a general recognition of the value that third-party data can bring to the fight against insurance fraud. To give an idea of range there is: intel from the IFB in the UK, CANATICS in Canada, national and state fraud bureaus in the US; there is information that credit bureaus hold; there is publicly available information such as electoral roll, unsatisfied Court judgements and bailiff searches. All of this data can be used to prove the identity of a customer, as well as being indicators of risk.

Continued over >

When it comes to data use, Insurers have historically been ahead of most other industries. They've always used data from outside their organisation. The challenge is the maturity with which they've then used that data analytically. There are so many opportunities to bring new data into the process; it can be difficult to find the value. The problem is not the availability of the data; it's often how you get from identifying the right data to getting value out of it fast. Insurers often pay every time they call out to data sources and that can get expensive, if they're not smart about it.

Q: Do you have any industry examples of this in practice?

A: We worked with a UK Insurer who wanted to analyse value from several external data sets to see which ones brought the most value. They also wanted to understand how they could gain maximum value from a single data set.

It was really important for them to be able to quickly validate genuine customersand remove them from the fraud process as quickly as possible. During the process 85 per cent of the individuals that appeared in claims and policies could be validated by the technology that BAE Systems provided, referencing third-party data sources such as Credit Referencing Agencies.

What we see typically with Insurers is they're often siloed. You'll have teams at the front-end of the business who care about selling policies, pricing the risk, risk selection. They care about getting the front-end right. Then, you get the claims teams at the back-end that care about keeping customers happy, preparing claims quickly and stopping fraud. This particular Insurer has tried to be more horizontal from a fraud perspective. It cut across what they're doing at the front end, what they do at the back end, and also what they do around financial crime, insider risk and compliance. The Insurer said it wanted one solution that best exploits all of their data, and third-party data, and it needed to take account of the front-end of the business. For example, are agents or brokers acting fraudulently? Are applicants fraudulent? Do claims contain fraud?

Q: Use of third-party data sources has data privacy implications. What is relevant here?

A: The growth of the digital and social media means there is more and more data an Insurer is able to gain insight from. There are however, regulatory issues that need to be thought through with the handling and use of this data, which is different in different regions. You need to make sure as an Insurer you are treating your customer's data with the care it deserves. You've got to be able to think sensibly about the terms and conditions under which that data is held. Many Insurers have a provision in their policy documents that any data provided to them can be used for counter-fraud purposes. The latest data protection regulations must be considered in relation to data collection, use and retention in existing processes and the design of new ones. Insurers also need to take into account the impact of their actions on public perception. Customers might be turned away by aggressive data collection or data use, as we saw last year, when Facebook blocked an insurer from adding data from its services to risk weightings. In relation to fraud though, proportionality is key. Insurers have to think about the balance between the proportionality of what they are using the data for, in terms of defending people from potentially serious criminal activity, and the invasion of privacy that comes with that.

85 per cent of the individuals that appeared in claims and policies could be validated by the technology that BAE Systems provided.

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

UK: +44 (0) 1483 816000

E: learn@baesystems.com | W: baesystems.com/businessdefence

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai