BAE SYSTEMS

Know your enemy

How insurers can understand the evolving threat of financial crime

Executive summary

Cate Wright,
Global Head of
Insurance Product,
BAE Systems.

"Corruption, embezzlement and fraud..." the former Chair of the US Federal Reserve, Alan Greenspan[1], once observed, are "the way human nature functions."

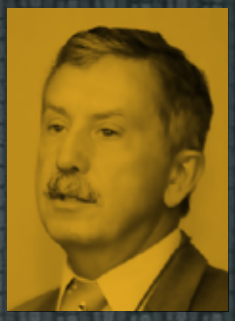
This rather defeatist approach to financial crime absolves criminals of responsibility. In the face of such a seemingly invincible enemy, insurers might just throw up their hands in defeat.

However that would be to miss real opportunities to tackle a growing problem. Fraud is perpetrated by a minority, thankfully; instinct is probably not the main cause. Therefore who or what is? How can insurers know their enemy?

Initially, we must unpick the motives for fraud - and why they outweigh the risks. Then we can look for perpetrators, study their tactics, and understand how criminal attacks against insurers fit into a broader criminal landscape.

The enemy is not one person[2]. Nor is there a sophisticated conspiracy against insurers. The financial criminal could be anyone[3]. By looking closely at reasons, methods and opportunities, we can assign classifications to those that attack insurance companies. With that insight, we can reduce the scale and impact of our enemies' threat.

[1] https://www.democracynow.org/2007/9/24/alan_greenspan_vs_naomi_klein_on
[2] https://www.baesystems.com/en/cybersecurity/feature/the-unusual-suspects
[3] https://www.baesystems.com/en/cybersecurity/feature/the-invisible-network



"I don't accept that fraud is part of human nature. It is a learned behaviour. If it was human nature, most people would be committing insurance fraud."

Dennis Jay, Executive Director of the Coalition Against Insurance Fraud.

Why does insurance fraud happen?

Dennis Jay, Executive Director of the Coalition Against Insurance Fraud, has dedicated more than 25 years to understanding, raising awareness of and fighting insurance fraud and its pernicious impact on society.

Since the early 1990s, the Coalition Against Insurance Fraud has been a leader in defending against insurance fraud in the US, playing an instrumental role in the introduction of anti-insurance fraud laws. These gave insurers the legislative teeth not only to prosecute fraud, but also to bring real deterrence into play.

With a legal framework in place, Jay and his Coalition colleagues turned to investigating the reasons for fraudulent behaviour.

"In 1997 we took a step back and commissioned what was at the time the most aggressive research on people's tolerance of fraud[4]," he says. "What we found was that 96 per cent of Americans fell into one of four categories: the moralists ('insurance fraud is wrong, period'); the realists ('insurance fraud will always be here and there is nothing we can do about it'); the conformists ('everyone else is doing it, so why can't I?') and the critics ('I have no problem with people sticking it to insurance companies')."

Finding these categories was a major breakthrough, says Jay, but a clear picture of which kinds of people were most likely to commit fraud continued to be elusive: "We could find very little distinction between the four groups in terms of age, geography, occupation, education. Fraud goes across all demographics."

[4] https://www.insurancefraud.org/downloads/Four_Faces_07.pdf

96% of Americans

fell into 1 of 4 categories

30% THE MORALISTS

'Insurance fraud is wrong, period'

21% THE REALISTS

'Insurance fraud will always be here and there is nothing we can do about it'

25% THE CONFORMISTS

'Everyone else is doing it, so why can't I?'

20% THE CRITICS

'I have no problem with people sticking it to insurance companies'

Source: Coalition Against Insurance Fraud, 2008 (1997 study) https://www.insurancefraud.org/downloads/Four_Faces_07.pdf

The peer pressure factor

One common theme did emerge – the effectiveness of peer pressure.
"For all of these four groups, peer pressure was by far the biggest influencer. Knowing how you would be viewed by your peers if you were caught committing fraud was the biggest motivator we found," he says.

Armed with this insight, the Coalition conducted several public awareness campaigns urging moralists and realists to speak up when they saw fraud and encouraging those considering it to think of the social implications of being caught.

Keen to understand the impact of their campaigns, the Coalition ran the same study in 2007[5] and 2017[6]. It wasn't until the latter piece of research that they started to see a shift.

The proportion of people who identified with the critic grouping had fallen from 26 per cent in 1997 to 11 per cent in 2017, while those willing to lie to claim for an uninsured loss had dropped from 93 per cent to 88 per cent. Even the proportion of those willing to 'finesse' a claim to get extra cash, had fallen from 91 per cent to 84 per cent. Bringing social pressure to play seemed to be having an impact.

"People tend to chuckle at insurance fraud compared with other crimes against companies. Our focus is, if you are in that situation, say something. You might understand why the person is committing fraud, but in doing so, your premiums are going to go up because that fraudster got a new iPhone," Jay says.

---

[5] https://www.insurancefraud.org/downloads/Four_Faces_07.pdf
[6] Coalition Against Insurance Fraud, 2017

Hazard warning
The accidental criminal

Fallen on hard times, the accidental criminal sees their insurance claim as an escape from a financial mess. Whether inflating the value of a genuine claim or inventing a loss, the accidental criminal feels fraud is no big deal, a one-off to get through a difficult period. It definitely won't happen again ...

Although the introduction of legislation directly targeting insurance fraud was a huge step forward, perhaps the Coalition's biggest success is this revelation that much of the fight against fraud is a battle for hearts and minds.

It is clear that the millions insurers spend every year on anti-fraud and IT security measures must be supplemented by real insight into who is committing fraud and why. Until we understand who the enemy is and why they are committing crime, we have little chance of finding them and even less of stopping them.

The insurer experience of crime

How insurers experience financial crime is complex. It cuts across both fraud and cyber attacks, is both organised and opportunistic and can arise internally and externally.

The picture may appear fragmented but in reality these are often different elements of the same crime.

As Simon Viney, Cyber Security Financial Services Sector Lead at BAE Systems, says: "An attacker can steal the data by a hack, then use that data to go for the fraud with the help of an insider to navigate the fraud checks."

To defend against this multi-faceted threat, insurers must understand both the identities – or type of identity – and possible motives of their enemies. Such insight will make the plan of action much clearer.

The weakest link

Insurers must identify where fraudsters are most likely to strike, and why. Cate Wright, Global Insurance Product Lead at BAE Systems, believes this is crucial: "For insurers there is a vulnerability at any touch point – be it at policy inception, mid-term adjustment, a claim or any supplier touch point."

A poorly protected supply chain is particularly attractive to fraudsters. Weak internal controls were a contributing factor in no less than three fifths of fraud cases in a 2016 KPMG survey of 750 convicted fraudsters for its Global Profiles of the Fraudster report[7].

[7] https://home.kpmg/content/dam/kpmg/pdf/2016/05/profiles-of-the-fraudster.pdf

Hazard warning
The criminal insider

A trusted team member with an exemplary service record, the criminal insider looks and acts like everyone else in the office – but poses a potent threat to your security. Either acting willingly, or coerced by a criminal gang, the criminal insider's focus is abetting an external attack by guiding external fraudsters through your defences. This type of criminal is more likely to be providing external criminals with company or customer data and security details than making an attack themselves.

Such vulnerabilities are exploited ruthlessly, often by industry insiders. Jorge Fausto Espinosa[8], who owned a loss-adjusting firm in Florida, was jailed for 20 years in 2018 after pleading guilty to racketeering, racketeering conspiracy, organised scheme to defraud, more than 28 counts of arson and multiple counts of insurance fraud and grand theft. The insider threat is clearly as much an issue in the supply chain as it is among employees.

Recruiting willing homeowners into his scheme, Espinosa set many homes on fire and flooded others to make $14 million of fake claims.

The network required was large, with police making 31 arrests.

Wright says that while vulnerability in supply chains is inherent and often unavoidable, it can be managed.

"Some insurers have fraud managers to manage and audit suppliers. They use data analytics to study every individual involved in the management of a claim and to identify whether a supplier is related to the claimant or vice versa," she says.

Supply chain risks are not limited to processing claims or purchasing. Data is one of an insurer's most attractive assets and the third parties involved in managing it must be monitored closely.

[8] https://www.miamiherald.com/news/local/crime/article211696869.html

Hazard warning
The fraud facilitator

Without this individual much fraud in the industry wouldn't be possible. Either part of an organised gang or acting alone, the fraud facilitator will carry out a cyber attack and feed the data to other gang members or sell it on to other criminals for them to commit more 'traditional' frauds against the insurer.

Hamish Karamsadkar, Senior Account Manager Banking and Insurance (Cyber) at BAE Systems Applied Intelligence, says: "Data storage is the main supply chain vulnerability, with firms using third parties to store or process data."

"A lot of my clients have started to develop security standards that are either their own or industry-recognised and this has become a prerequisite to working with the insurer."

Identifying weak points, however, is only useful if you know who is targeting them and how.

Know thine enemy

Now we understand the weakest link in an insurer's defences, can we build a definitive profile of those who might attack it?

Scott Clayton, Head of Claims Fraud at Zurich UK, urges insurers not to limit their search. "Fraud is motivated by greed, need or jealousy and those traits can apply to anyone. We have seen them from all ages, backgrounds, financial standing and location," he says. "There is no stereotypical fraudster."

Clearly profiles must be nuanced and sophisticated, given the lack of real insight. A 2015 study by Professor Martin Gill and Amy Randall[9] for the Association of British Insurers found that although there was a broad range of types of insurance fraud, insight into the fraudster's perspective was lacking or entirely absent – in short, it could be anyone.

[9] https://www.abi.org.uk/globalassets/sitecore/files/documents/publications/public/2015/fraud/insurance-fraudsters-a-study-for-the-abi.pdf

Hazard warning
The former employee

Previously a cultural risk in the office, the former employee can turn into a physical security risk. This can come in a number of ways – from downloading and removing customer data to writing 'logic bomb' malware into software to be triggered when they choose. They may be out the door, but their threat remains.

While research into fraudsters may be thin on the ground, there are pointers to help insurers narrow the field and start to profile the most likely offenders.

In its Global Profiles of the Fraudster[10] report, KPMG found that 79 per cent of fraudsters were male; 68 per cent were aged between 36 and 55; 65 per cent were employed by the victim organisation, with a further 21 per cent being former employees.

Interestingly, the study found that fraud is almost twice as likely to be carried out in groups rather than by individuals acting alone. These groups very often comprise both insiders and outsiders.

Stephan Drolet, National Forensic Leader, KPMG in Canada, said in the report: "Companies have to design anti-fraud mechanisms that look both ways, inside and outside. They need to be aware of the possibility that a lone, inside fraudster may be working with a sizeable group of people on the outside."

This might only scratch the surface of a fraudster's identity, but it is important to identify the two main perpetrators – organised gangs and opportunists.

What do we know about their motivation? While money may seem obvious for both camps, closer inspection throws up revealing nuances.

Organised criminals want money, pure and simple. Attacks against insurers are often just one part of their wider criminal operations.

[10] https://home.kpmg/content/dam/kpmg/pdf/2016/05/profiles-of-the-fraudster.pdf

Hazard warning
The organised criminal

Insurance fraud is probably just one of several strings to the organised criminal's bow. They might be running a crash-for-cash ring, a team of hackers, or be involved in drugs trade, people trafficking or any other criminal enterprise[11]. Insurance isn't the attraction. Access to data and cash – and lack of defences – is the main motivation.

In 2017, Mohammed Sangak[12] was jailed at Maidstone Crown Court for 10 years for running a crash-for-cash scam that netted hundreds of thousands of pounds. The boundaries of Sangak's criminal enterprise stretched far beyond insurance. He was also convicted of plotting to smuggle illegal immigrants into the UK.

In America, Philadelphia auto bodyshop owner, Ron Galati Sr.[13] was sentenced in 2016 to up 29 years in prison for defrauding insurance companies (with 40 other co-conspirators) out of nearly $2 million through motor fraud.

Again, insurance fraud was not his sole criminal enterprise. When convicted, he was already in jail for multiple murder-for-hire plots.

With the opportunistic fraudster, money is, of course, the motivation but, unlike with established criminals, the drive to commit a crime doesn't come naturally. It requires other prompts and social permissions.

---

[11] https://www.telegraph.co.uk/news/2019/04/15/italian-police-arrest-gang-broke-victims-limbs-iron-concrete/

[12] https://www.kentonline.co.uk/medway/news/alleged-car-crash-fraudster-made-123498/

[13] https://www.metro.us/philadelphia/ronald-galati-sentenced-to-lengthy-term-for-insurance-scams-son-receives-home-confinement/zsJpli---bXyzJhSjnbshk

Hazard warning
The habitual opportunist

This individual often evolves from the accidental criminal. Having got away with fraud once, the habitual opportunist sees the possibility of regular, guilt-free income and looks for new methods and new companies to defraud. What started as a one-off has become a habit but, for now at least, remains a part-time pursuit.

In 1953, the American criminologist Donald Cressey conceived the Fraud Triangle[14], which identifies three factors leading to fraud and other unethical behaviour.

- **Pressure** – such as money problems, gambling debts, alcohol or drug addiction

- **Opportunity** – a low likelihood of being caught or the ease of discovering vulnerabilities in a company's processes

- **Rationalisation** – justification of their actions, such as believing defrauding a large company is a victimless crime

Insurers can do little about the first factor – pressure, but opportunity and rationalisation are very much open to influence. It is by addressing structural weaknesses and challenging public attitudes towards insurance fraud that insurers have the best chance of success.

Creating the stigma

"With commerce, comes fraud," according to Nathan Blecharczyk, co-founder of AirBnB[15]. And one reason opportunistic fraud remains such a stubborn problem is that many people don't consider it a big deal.

Cate Wright believes it is often socially acceptable: "There is a lot of peer pressure to commit insurance fraud and it is accepted socially. People would be disgusted if somebody smoked in a pub, but everyone laughs about insurance fraud."

She argues that one of the most effective ways to challenge this attitude is to stigmatise it by making plain the association between fraud and serious organised fraud.

---

[14] https://www.brumellgroup.com/news/the-fraud-triangle-theory/

[15] https://medium.com/airbnb-engineering/hard-problems-big-opportunity-4e1fac7fe75e

Although insurance fraud's place in the broader criminal landscape remains unclear, the reach and complexity of global organised crime makes it inevitable that insurance fraud is part of a bigger picture.

Jon Draper, Product Strategist, Futures at BAE Systems, explains: "If you look at the global trade system, it is super-complicated. Trillions and trillions of dollars are going through ports and containers in a mind-bendingly complex trade system. But nobody designed it – it evolved.

"And the global crime system has evolved in line with global trade. A massive chunk of global trade is criminal with a trillion dollars of proceeds going through the system every year."

The evolution of global trade has been matched step by step, he argues, by the evolution of global criminal interactions.

"As small companies trade online globally as part of the worldwide trade network, so to do criminal gangs. The connections between the small and the big criminal players are hugely intricate," he says. "Criminals of all shapes and sizes are trading with each other, just as businesses are."

It may be difficult to provide clear evidence that insurance fraud fits into a wider criminal system, but there are enough indicators to suggest it does.

If insurers work to establish and expose the links between insurance fraud and far more serious crimes, they can build that much-needed stigma around insurance fraud.

Building robust defences

There is little point trying to convince organised criminals that their actions are wrong. The focus must be on deterrence and defence, and this must bring the anti-fraud and cyber security communities together.

Simon Viney believes this joined-up approach is key. "Too often we see the fraud team identifying a threat or an attempt to defraud, unaware of the cyber element of the fraud."

"They won't tell the cyber team what they are investigating, when often the two are investigating two elements of the same crime."

Modern crime is so intricate that an organised fraudster seldom acts alone or against just one insurance company. This makes interaction between different divisions within an insurance company crucial to the fight against organised fraud. This difficulty is multiplied when looking at how companies might work together.

With opportunistic fraud, the path seems clearer. Cressey's triangle identifies two clear areas where insurers can make inroads – opportunity and rationalisation.

An insurance company that lacks robust defences is inviting fraudsters to have a go. Remove the opportunity and you remove a key cause of fraud.

As the 2015 ABI study[16] recommends: "Where fraudsters weigh up the pros and cons there is the opportunity to influence their decision-making by rendering a fraud act as less attractive, by for example making the offence more risky."

Alongside that, insurers must challenge the perception that committing insurance fraud is acceptable. After all, few outside the criminal fraternity would want to be associated with drug traders or people traffickers.

Conclusion

As the Coalition Against Insurance Fraud has shown in America, by creating unambiguous associations with the more extreme elements of insurance fraud, organisations can start to shift the perception dial.

At present, social pressure aids insurance fraud. Targeted, consistent public messages can flip that over, applying peer pressure that ensures insurance fraud in all its guises is seen as the social and financial menace that it really is.

[16] https://www.abi.org.uk/globalassets/sitecore/files/documents/publications/public/2015/fraud/insurance-fraudsters-a-study-for-the-abi.pdf

What next?

A well-structured organisation is the foundation of a robust defence against insurance fraudsters. Start by identifying the skills, capability and technology you already possess.

Break down walls

All too often internal expertise that could be put to use to identify threats is not applied to the problem. This is all the more troublesome if resources are tight, demand for the skills of teams or individuals is in high demand, or siloed in organisational fiefdoms. You can find out more about how to do this at baesystems.com/problem-shared

Borrow data science and analytics skills

Data scientists are a scarce resource – and as a result often in high demand. Third-party analytics services work as a force multiplier for in-house teams. In-house analytics teams can be used to direct capability rather than doing all the legwork themselves. Look out for our report on this topic at baesystems.com/insuranceinsights

Share resources and techniques across lines of business

It's likely that one part of your organisation has significant counter-fraud resources at its disposal that could benefit other lines of business; more than one insurer has dedicated significant resource to tackling motor fraud – and the lessons learnt, expertise developed and systems built can often be transferred, in whole or part, to other lines.

For more information go to: **www.baesystems.com/insuranceinsights**

Contact us

E: learn@baesystems.com
W: baesystems.com/insuranceinsights

Victim of a cyber attack? Contact our emergency response team on:

US: 1 (800) 417-2155
UK: 0808 168 6647
Australia: 1800 825 411
International: +44 1483 817491
E: cyberresponse@baesystems.com

linkedin.com/company/baesystemsai

twitter.com/baesystems_ai

BAE SYSTEMS