BAE SYSTEMS

Insurance fraud trends in 2020

Much the same, yet completely new

INSURANCE INSIGHTS
FROM BAE SYSTEMS

Discover the best practices insurance leaders can take to counter the evolving, evasive world of financial services fraud as we begin a new decade.

The world in 2020 is an unusual and unpredictable place. The insurance market was set to hit new highs this year. Then COVID-19 happened. That forecast – and the global economic outlook – is now far less certain as a result.

The uncertain insurance future

BAE Systems' Dennis Toomey referred to this in a recent blog post[1]. And the impact of the global health crisis on the insurance sector has been noted by Deloitte too[2]. "Insurers across the board would likely be impacted by a sharp slowdown in economic activity, which would undermine growth and perhaps even contract insurable exposures... Financially, insurers will also likely need to adjust their budgets and implementation plans, cash flow expectations, and investment portfolios in light of recent developments."

But while market growth projections are in a state of flux, the rate (and evolution) of fraud isn't expected to slow down. Insurance fraud is anticipated to cause $80–$100 billion in lost revenue this year.[3]

Fraud is sometimes seen as a victimless crime – liberating what appear to be small amounts of money (in isolation) from firms that can apparently stomach the losses.

The trouble is, fraud isn't a victimless crime.

It can fund organised criminal activity. It's often a central vehicle for money launderers. Its proceeds are even used to fuel terrorism.

Dennis Toomey recently attended the Global Insurance Fraud Summit, which brought together 50 industry experts from 16 countries – including law enforcement, regulators, fraud and insurance crime bureaus, national consortiums and fraud departments. The summit aimed to develop a comprehensive vision and plan to tackle global insurance fraud – the first step of which involves coming up with an internationally recognised and adopted definition of fraud. The output from the summit will be shared with organisations around the world to help increase collaboration, and share best practices.

As insurers seek to understand, respond and ultimately clamp down on fraud, there are five key trends they need to be aware of. This Insurance Insights report explores these trends and explains how insurance leaders can adapt as fraud evolves.

[1] https://www2.deloitte.com/uk/en/insights/economy/covid-19/impact-of-covid-19-on-insurers.html

[2] https://www2.deloitte.com/uk/en/insights/economy/covid-19/impact-of-covid-19-on-insurers.html

[3] https://www.insurancefraud.org/statistics.htm and https://www.justice.gov/archives/jm/criminal-resource-manual-976-health-care-fraud-generally

Trend #1: The new era of fraud investigation

Modern fraud is transnational and agile. So, it follows that the insurance industry can't rely on traditional techniques to combat what is an evolving enigma.

Not so long ago, fraud investigation was a labour-intensive process. Teams on the ground would literally go door to door to examine cases. Today, this process isn't just inefficient – it's insufficient.

As fraud evolves, so must investigators. It's time for a new breed of insurance investigator. Today's fraud fighters need nuanced skillsets and agile ways of working to be able to identify the scams and tactics modern fraudsters are adopting.

But they must also strike a delicate balance. Because, while investigators need to gather data and build a case that will result in criminal prosecutions, they must also consider privacy implications that are more stringent than ever before.

In the age of GDPR and the California Consumer Privacy Act, it's not just a new era for insurance investigation, but a new era for evidence collection too.

A number of questions need to be addressed. How long can you store data for? What are the implications for data privacy? How do insurers gather evidence while staying on the right side of regulatory drivers?

The gold standard is intelligent actionable evidence collection. But with the battle for privacy fiercer than ever – and international institutions protecting individuals – that's easier said than done.

While today's investigators have more tools at their disposal, they also face more onerous demands and more sophisticated fraud techniques than ever before.

Trend #2: The significance of social media

Building on our first trend, today's investigators must also acknowledge the central role that social media plays as a primary source of intelligence. Mining social media for information to uncover otherwise hidden relationships and connections between entities is already vital to the counter fraud engine of many insurers – delivering greater insight as well as improved investigation efficiency, automating large parts of the process.

Leading insurers are placing huge value on social media, with many carriers having a dedicated team of social media analysts. But while human expertise will always be critical, the uptake of automation and artificial intelligence is accelerating.

A range of tools exist to automate social media investigations. So, the challenge isn't the availability of the technology, but the compatibility and stability of the platform.

Born out of our engineering heritage, BAE Systems' tools are able to sift through social media content and unearth evidence of potential fraud. This crunches data processing down from days to minutes. API compatibility is important too – giving our customers the ability to use any data source and integrate tools seamlessly into their environments.

Trend #3: Converging fraud and risk calls for the collapse of silos

Until recently, fraud scams were fairly rudimentary. Fraudsters would steal an identity, create synthetic IDs and execute criminal activity. It was a repeatable, linear and somewhat predictable process.

Today, criminals are more subtle and nuanced in their approach. They might wait for initial surveillance to conclude and then execute their attacks knowing that a previously obtained synthetic ID is less likely to trigger alarm bells. They may stage accidents, perhaps using technology to make their shams appear more legitimate. Or they might use cryptocurrencies to hide payments and transfers.

Insurers need to be alert to the risk that certain entities and transactions carry as fraudsters seek to expose new channels and adopt new tactics.

One area that insurers need to be particularly conscious of is silos. Whether they're within departments or interdepartmental (between cyber and risk divisions), silos enable fraudsters to execute their scams.

Obfuscation and obstacles between departments have traditionally been exploited by fraudsters, who know they can conceal information to evade investigators. That's why insurers are now moving to embrace a 360-degree view of fraud, breaking down the silos that previously obscured suspicious activity. Accordingly, insurance carriers understand that they need to manage their data differently to be able to identify and thwart fraud.

Trend #4: The crucial role of consortiums

The value that consortiums offer the insurance industry is increasing. They provide a bird's eye view of transactions and shine a spotlight on suspicious activity across multiple carriers and lines of business.

Currently, the maturity of insurance consortiums varies between regions and countries. Organisations like CANATICS in Canada are already adept at analysing cross-carrier activity and providing invaluable surveillance intel. In the US, the state of Massachusetts has one of the most sophisticated consortiums, and there are now plans to introduce this model to New York State.

BAE Systems currently works with three consortiums, bringing data from different financial services sectors to create a comprehensive picture of criminal financing and money laundering.

Trend #5: More insurance lines = more fraud variety

As more insurance products are introduced, the surface area for insurance fraud grows. Fraudsters seek to adapt and exploit the volume and variety that those proliferating insurance lines offer.

Both existing and new insurance products are under threat. Just consider two of the most established lines.

Life insurance can be gamed by entering incorrect details during the application phase to avoid high premiums. Meanwhile, healthcare insurance can be manipulated by masking existing or underlying conditions.

Newer products are also targeted. In the US, workers' compensation insurance is subject to mod factor gaming. Higher salaries are hidden, shell companies are created and employee classifications are massaged (changing job titles, for example) to bring premiums down.[3]

Larger more established companies entering into these new lines can afford to fight emerging fraud techniques. Sadly, smaller niche firms can't – and they're often the ones fraudsters target.

Staying ahead of the fraud frontiers

Fraud is constantly changing. Paradoxically, that's the one thing about fraud that never changes. And as this pernicious practice evolves, carriers need a partner with a track record of anticipating trends and evolving faster than fraudsters.

BAE Systems has the human expertise and machine intelligence to help you stay steps ahead of insurance fraud. Find out more about how we help leading insurers across the globe to thwart fraudsters and serve genuine customers more effectively.

[4] http://insurancemarketsource.com/buildyourbusiness/3-types-of-insurance-premium-fraud-and-how-to-detect-it/

Explore our range of resources and further reading

- Read the Blog: fraud thrives in a crisis – why the insurance community needs to stay vigilant
- Listen to the podcasts: the insurance pandemic – fighting fraud in lockdown with Tony DiPaolo, Executive Director of the Massachusetts Insurance Fraud Bureau and Matthew Smith, Director of the Coalition Against Insurance Fraud discusses insurance fraud risk and opportunity
- Discover: our insurance fraud solutions
- Explore: The Intelligence Network's tackling cyber fraud vision paper

About Dennis Toomey

Global Director, Counter Fraud Analytics and Insurance Solutions

Dennis brings nearly three decades of experience to BAE Systems' Insurance team. A Certified Fraud Examiner in the US, Dennis has held senior positions at SAS, Accenture, the Security Intelligence Insurance Practice, Liberty Mutual and LexisNexis. He holds an MBA from Franklin Pierce University.

Contact Dennis

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK
E: learn@baesystems.com | W: baesystems.com/insuranceinsights
linkedin.com/company/baesystemsai
twitter.com/baesystems_ai