Coming together to combat digital fraud

Time for a New Era of Insurance Fraud Investigation?
The global pandemic we now find ourselves in has created rapid and unparalleled shifts in the way we live and work. Unfortunately, as is so often the case, fraudsters have been among the quickest to exploit these changes. They’re increasingly moving online, utilising sophisticated techniques to stay hidden, impersonate legitimate customers, and file false insurance claims.

There will be no return to “normal” anytime soon, if ever. As Wellcome Trust director, Jeremy Farrar, told UK MPs recently, even if a COVID–19 vaccine is found "humanity will still be living with this virus for very many, many years ... decades to come." It’s therefore time for insurers to adapt to the new reality: to understand fast-evolving fraud patterns and develop effective mitigation strategies. These will need to include a greater focus on information sharing: across departmental siloes, businesses and geographical boundaries.

In this Insights paper, Dennis Toomey, Global Director of Counter Fraud Analytics and Operations for BAE Systems takes a look in more detail at the scale of the problem facing the insurance sector, and suggests some of the ways we can tackle it.
Digital transformation means digital fraud

Technology may be empowering organisations to support mass remote working, adapt their business models and stay connected with customers during the pandemic, but it is also underwriting a new wave of cyber-enabled fraud. The roots of this go back long before the pandemic began.

The unstoppable rise of digital transformation has created the perfect storm for such fraud to thrive. As businesses shift more of their operations online to enhance the customer experience, cut costs and deliver innovative new services, they’re capturing more and more of their customers’ data. Lapses in corporate cybersecurity means this information increasingly ends up on underground trading sites, where it is bought and used by scammers to impersonate these customers, or create synthetic identities, perhaps by submitting false claims.

Some 8.4 billion records are estimated to have been exposed in the first quarter of 2020 alone – a 273% increase compared to Q1 2019. That’s a lot of possible information for fraudsters to use.

More specifically, COVID-19 has created the conditions for several emerging threats to insurers:

1. Taking advantage of fewer at-scene investigations, fraudsters have been submitting false claims for thefts, damage to property (i.e. house and garage fires), personal injury/accidents and other claims that are hard to verify remotely. Tell-tale signs are sudden increases in house contents values, or incidents where fires are put out/accidents happen without the emergency services being called.

2. Fraudulent compensation claims against companies just before they go bankrupt, making it problematic for investigators to obtain the information they need.

3. Telemedicine is in vogue as an important way for patients to seek medical help without exposing themselves or others to potential COVID-19 infection. However, it opens the door to a range of fraudulent activity. Impoverished healthcare providers could invent appointments, diagnoses and prescriptions with the aim of getting reimbursed by insurers. Unscrupulous telemedicine companies may trick patients into buying medical equipment or prescriptions they don’t need in scams which have become increasingly complex and transnational. While some such schemes are reported to have been dismantled, some estimates suggest healthcare fraud in the US continues to cost the industry as much as $300 billion annually.

The bottom line is this: today’s cyber-criminals are more sophisticated than before, often tailoring their tactics for each individual scam. They may perform reconnaissance on their targets to improve chances of success. They may also use anonymizing browsing tools and cryptocurrency to stay hidden and launder money more efficiently. This puts the pressure on modern fraud fighters.
A new era of insurance fraud investigation

Adding to this pressure is the barrier to effective fraud prevention represented by organisational siloes. These may occur between internal and external fraud teams, underwriting and compliance teams, especially within international organizations with data silos set up geographically. These silos can allow fraud to flourish in the absence of holistic entity resolution and internal intelligence sharing network analytics.

Information is power, and in this case, money: with the right tools and strategy along with a 360 degree view of the entities within their data, insurers could save themselves and their customers significant sums both from a fiscal and reputational perspective.

The good news is that connected technologies - not limited by social distancing guidelines - are already here to make this a reality. Cutting-edge forward thinking technologies include:

- **Voice analytic/biometrics** to spot fraud via phone interviews with insureds or claimants
- **Geospatial mapping, satellite imagery and analytics** to assist in remote investigations and evidence collection
- **Document and image analytics** to identify potentially fraudulent photos and altered or forged invoices
- **Automated social media mining** to uncover hidden relationships and connections between entities
- **Homomorphic encryption** to allow organizations the ability to securely collaborate across the industry, business lines, and international borders
So-called cross industry fusion centres might increasingly offer another great way to detect and deter financial crime by tackling the manual, siloed, reactive way the financial services industry has historically addressed fraud and intelligence.

These fusion centers typically bring together experts from fraud, cybersecurity, threat intelligence, risk and other key stakeholders across the financial crime industry to share insights and begin to assemble that 360-degree view of suspicious activity across multiple channels and domains. The ultimate goal is what McKinsey describes as “strategic prevention” — the ability to predict rather than merely react to fraud risk.

However, info-sharing efforts must also ensure data is effectively protected, managed and anonymised to comply with GDPR, CCPA and other privacy regulations. The ability to share law enforcement intelligence and data with the private financial services industry has always been a challenge. Fusion centers with the right analytic solutions and architecture can ensure compliance and the data and information is only shared with those authorized to see and use it. This will require close co-operation not only between fraud and risk teams but also compliance and public agencies.
Coming together

Although individual insurers can avail themselves of such technologies and tactics to improve their ability to detect sophisticated fraud, we also need action on a broader scale to effect real change.

Information sharing needs to happen not just within organisations but between them, and law enforcement. Industry consortiums like Canada’s CANATICS are crucial here, as are initiatives like The Intelligence Network, launched by BAE Systems two years ago and now boasting more than 2,000 members.

Industry events, like last year’s BAE Systems hosted Global Insurance Fraud Summit (GIFS) brought more than 50 industry representatives from 16 countries to share best practices. The virtual 2020 conference is expected to double the size and address international issues relating to Transnational Insurance Fraud Trends. GIFS is co-Sponsored by the National Insurance Crime Bureau (NICB), International Association of Special Investigation Units (IASIU) and the Coalition Against Insurance Fraud (CAIF).

The fight against insurance fraud is not simply a matter for the insurance industry. The repercussions of this multibillion-pound threat on global GDP, organised crime, policyholder premiums and even taxation rates are immense. However, there’s no silver bullet solution to the problem. As an industry, we need to become as agile and tech-savvy as our opponents, prepared to collaborate closely with our colleagues in compliance and risk roles as well as the wider sector.

As COVID-19 continues to disrupt the old ways of doing things, so must we.
About the author

Dennis Toomey
Global Director of Counter Fraud Analytics and Operations

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.

Recommended content:

READ THE BLOG
Fraud thrives in a crisis – why the insurance community needs to stay vigilant

LISTEN TO THE PODCAST
Renato Schipani, Criminal Intelligence Officer from INTERPOL discusses transnational organised crime and transnational insurance fraud

LEARN
About the latest insurance fraud trends for 2020

DISCOVER
Our insurance fraud solutions

---

1 Humanity will be living with the coronavirus for “many years,” says health charity chief, Michael Le Page, Clare Wilson, Jessica Hamzelou, Adam Vaughan, Conrad Quilty-Harper and Layal Liverpool, New Scientist (21 July, 2020)
2 2020 Q1 Data Breach QuickView Report, RiskBased Security (May 11, 2020)
3 The Challenge of Health Care Fraud, NHCAA, (accessed July 27 2020)
4 Financial crime and fraud in the age of cybersecurity, Salim Hasham, Shoan Joshi, and Daniel Mikkelsen, McKinsey (October 1, 2019)
At BAE Systems, we provide some of the world’s most advanced technology defence, aerospace and security solutions.

We employ a skilled workforce of 82,500 people in over 40 countries. Working with customers and local partners, our products and services deliver military capability, protect people and national security, and keep critical information and infrastructure secure.