SHIFT

SHIFT TECHNOLOGY INSURANCE PERSPECTIVES

THE DIGITAL FRAUD TRENDS EDITION

www.shift-technology.com

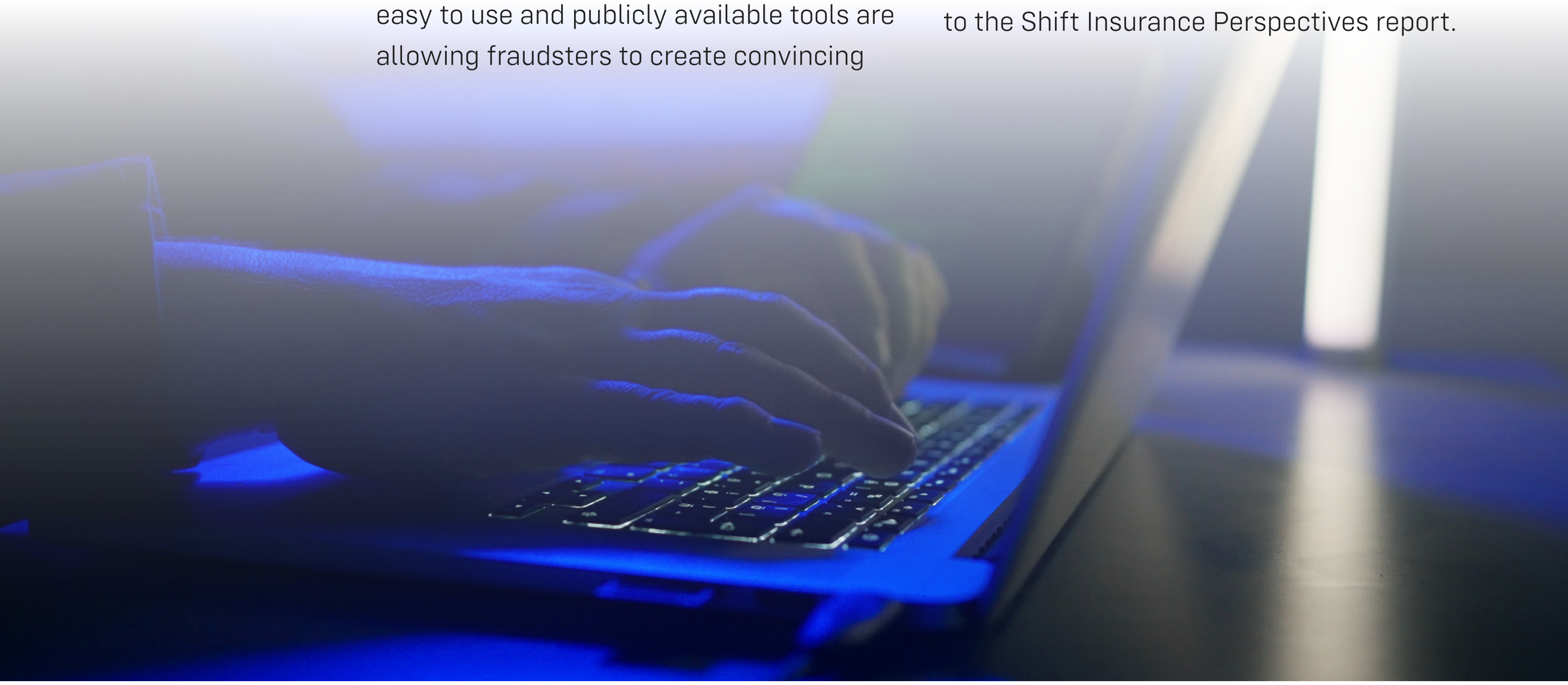
From the editor

Artificial Intelligence (AI), and more specifically Generative AI (GenAI), have captured the attention of businesses and consumers alike. For insurers, these technologies are supporting and improving processes such as claims and underwriting, among many others, that are critical to ongoing business success. Artificial intelligence is driving efficiency gains and helping insurers bridge the talent gap being created by a disparity in the number of employees leaving the industry versus those entering it. These powerful solutions are helping insurers see the big picture, make the best decisions possible, and shave points off of combined ratios.

At the same time, the very same tools that are delivering tremendous benefits to the insurance industry are also creating a whole new set of risks. Bad actors are using AI and GenAI to invent new fraud schemes. They are using these technologies to make existing schemes harder to detect. And easy to use and publicly available tools are allowing fraudsters to create convincing photos, documents and other "evidence" required to establish illegitimate policies and falsified claims. The age of the "insurance deep fake" is upon us.

In this edition of Shift Insurance Perspectives we will explore some of the ways in which AI and GenAI are being used to drive advances in digital fraud aimed at the insurance industry. How did a desire to create more opportunities for customer self-service and less human intervention from insurers open the door to more fraud? What do new digital schemes look like and how are they exploiting existing gaps in anti-fraud strategies? Where is AI and GenAI being used by bad actors? And perhaps most important, how can AI and GenAI be used by insurers in the fight against underwriting and claims fraud?

As always, this report is only possible based on the combined talents of many Shift employees across the organization. Thank you for your continued contributions to the Shift Insurance Perspectives report.



Policy fraud networks

Consumers celebrated when the insurance industry began adopting the digital advances they had become accustomed to through online and mobile commerce. Unfortunately, so to did the bad actors looking to take advantage of the system. The ability to apply for coverage online, without requiring human intervention, meant prospective policyholders could now shop for insurance the same way they shopped for almost everything else in their lives. Using an online portal or app was fast, convenient, and efficient. The same held true for the claims process and the move toward “no touch, low touch” and straight through processing (STP) initiatives. For insurers, embracing digital approaches meant their experienced brokers, underwriters, and claims professionals could spend time on the more complicated applications and claims where their expertise was required.

> **For those looking to defraud the industry, removing the human element from underwriting and claims has effectively created new opportunities for large scale fraud.**

For those looking to defraud the industry, removing the human element from underwriting and claims has effectively created new opportunities for large scale fraud. Many of these schemes hinge on the use of stolen identities and fraudulent documents to obtain illegitimate policies. Let us examine a recent example of a policy fraud network identified by Shift that comprised 146 new policies generated over the course of six months. These policies covered higher value vehicles and the corresponding drivers all showed a clean record. The reality, however, was far different. The insurer in this situation subsequently faced a number of third-party claims against those policies. While none were significant enough to raise a red flag individually, the policy fraud network generated costs to the insurer that reached into the hundreds of thousands of dollars. This is why AI is so important in fighting this type of digital enabled fraud.

In this situation, AI-powered entity resolution is the first step in identifying a policy fraud network before significant damage is done. Analysis of policy and claims data identifies similarities in the information provided that may not be easily noticed when looking at individual applications or claims. Once those connections are identified, it becomes easier for insurers to take action against the network. Remedies may include automatically investigating claims associated with the network, routing policies for non-renewal, and carefully reviewing applications suspected to be part of a network.

Spotting false declarations

Insurers have been dealing with false declarations for nearly as long as there has been insurance. In the effort to gain better premiums, applicants may be tempted to provide information about themselves, their vehicles, or their property that paints their application in the best light possible. For individuals, this may mean under-reporting the number of miles driven per year or listing a more desirable address for where a vehicle is permanently garaged. Or It may mean neglecting to notify that a vehicle or part of the home is being used for business or commercial purposes. These seemingly small inconsistencies have the very real potential to lead to significant premium leakage and future claims costs.

But what happens when making false declarations happens at scale? Premium leakage and associated claims costs can rise exponentially. Shift has seen examples of the ways in which dishonest businesses can use false declarations to create real problems for insurers. In one particular case, a single address in a desirable neighborhood was associated with more than 10 different vehicles all identified as being solely for personal use. This facade hid the fact that none of the vehicles were actually garaged at the address provided in the application. As important, all of the vehicles were being used for commercial purposes. Had this not been uncovered, the insurer stood to lose tens of thousands of dollars in increased claims costs in the event of an incident.

With false declarations and false declaration networks we find another fraud scheme enabled by insurers' move to more digital interactions, but also highly susceptible to being discovered through adoption of AI-powered fraud and risk detection solutions. Entity resolution and network detection is able to analyze applications and existing policies for shared information such as phone numbers and email addresses. Including third-party data into the analysis, such as business and other public records, as well publicly available social media can help determine the true nature of who is behind the policy (e.g. is it a business entity or an individual).

Digitally assisted ghost broking

Ghost Broking can be perpetrated by both licensed agents who sell policies and pocket the premiums without actually insuring policyholders or unlicensed "agents" who sell fraudulent policies to customers. We are examining the latter in this report. This type of scheme specifically targets those individuals seeking inexpensive insurance or whose premiums may be negatively impacted due to claim history, location, age, or other factors. The ability of bad actors to digitally manipulate the documentation supporting an application or policy has led to an increase in this type of fraud.

In Shift's own work related to Ghost Broking networks operating in the UK, insurers have uncovered networks with as many as 400 policies impacted.

A recent example that was reported in Italy highlights the methods by which fraudulent brokers profit. Criminals acting as insurance agents used both stolen identities and the identities of deceased individuals to purchase inexpensive policies through false declaration. These policies were then sold to unsuspecting consumers. Forged vehicle sale documentation made it appear as though it was the new policyholder's vehicle on the insurance policy. The fraudulent broker pockets the difference in premiums. In the event of an incident, the broker disappears, leaving the insurer on the hook to settle the claim.

It was estimated the cost to insurers impacted by the Italian scheme was more than 700,000€, with 274 people suspected of participating in the fraud. In Shift's own work related to Ghost Broking networks operating in the UK, insurers have uncovered networks with as many as 400 policies impacted. This represents the potential for hundreds of thousands in losses in each network.

Much like other forms of policy fraud, AI is critical to uncovering and stopping this type of Ghost Broking. The ability to spot network links through the proliferation of identical banking information, contact information, or other PII across policies is fundamental. Insurers who can do this are well equipped to identify network links associated with new applications in real time, helping to keep these fraudulently booked applications from becoming policies.

Using AI to help commit fraud

As AI and GenAI tools became widely available online and easy to consume by novices and experts alike, their usefulness to bad actors quickly became apparent. Rapid advances in GenAI more particularly have made it much easier to create convincing images and supporting documentation for use in policy or claims fraud scenarios. Fraudsters can produce photos showing extensive damage to a vehicle or home. They can create or manipulate documents including police reports, invoices, or estimates, among many others. To the human eye, these "insurance deep fakes" are difficult to discern from the legitimate documents and images required to support a policy application or a first notice of loss (FNOL). And while organizations like the Coalition for Content Provenance and Authenticity (C2PA) are taking steps to make it easier to identify AI-generated images and documents, its existence alone will not solve the problem. Not only are there an untold number of documents and images already created and in the wild, but also there will always be technologies available from vendors or open source channels that do not participate in industry self regulation.

This is where AI can play an important role in defeating digital fraud. Entity resolution and network detection can again be used to identify common PII and other forms of data in manipulated or created documents, raising a red flag that there is something suspicious happening in the underwriting or claims process. As important, AI-powered image and document analysis is able to quickly, efficiently and accurately identify image aberrations, metadata abnormalities, or other indicators of generative AI-based fraud schemes and identify related policies or claims as in need of further review or investigation.

Conclusion

The digital revolution opened incredible opportunities for insurers to do business in a way more directly aligned to their customers' needs. Adopting online commerce models and "anywhere, anytime" access created new efficiencies and conveniences for carriers and their customers. However, removing human interaction from certain transactions opened the door for bad actors to take advantage of the new normal. The digital tools empowering the insurance revolution were actively being used against the industry to commit fraud. But savvy insurers are onto these new schemes and using AI-powered solutions to spot, and stop digital insurance fraud in its tracks.