SEPTEMBER 2020

ARTIFICIAL INTELLIGENCE & INSURANCE FRAUD

Decoding the mysteries of AI for the fraud-fighting community

In conjunction with:

Coalition Against Insurance Fraud

Shift
The term Artificial Intelligence — or AI — has become a “catch-all” buzzword in recent years. A consequence of this trend is confusion about what constitutes “true” AI and its role in combating insurance fraud. Yet, AI is not new. The technology first emerged in the early 1970s and has been applied to several aspects of technology over the past few decades. And during those years, an ever-increasing availability of data, and the computing power required to effectively analyze it, have fueled the hype and hopes the fraud-fighting community is witnessing today. Yet many consumer advocates, and justifiably so, are concerned. AI presents both exciting opportunities together with potential risks for everyone involved.

For insurance executives and SIU professionals in particular, the AI landscape has become increasingly confusing. These professionals are bombarded with terms such as machine learning, natural language processing, supervised and unsupervised learning and image recognition, to name but a few. But those terms provide little context to how these technologies differ or how they impact claims and other fraud-detection processes.

This report seeks to help explain the differences in the various technologies and AI techniques used to detect insurance fraud. The study includes the findings from an online survey of 30 insurers representing a significant share of the property/casualty insurance market. In addition this report includes comments from interviews with several leading insurers that have successfully implemented AI into their anti-fraud technology.

Finally, this report includes a brief outline of some of the public policy issues relating to the use of AI in insurance. While most do not directly impact the use of AI in fraud detection, they may be useful in supporting a better overall understanding of the broader use of AI in insurance.
EMPLOYING ARTIFICIAL INTELLIGENCE TO DETECT INSURANCE FRAUD
Understanding AI

For this report and the accompanying survey results, AI is defined as a data technology solution that systematically screens for questionable claims using predictive analytics logic driven by advanced data modelling techniques and statistical algorithms.

Interestingly, the perception that AI is new to the arsenal of tools to combat insurance fraud was debunked by the results of the survey. A majority of insurers (56%) indicated that their company was using AI in one form or another for fraud detection, and have been doing so for quite some time.

Among other key findings

- More than 30 percent of insurance executives surveyed expect the COVID-19 pandemic to drive an increase in the use of AI to fight fraud.

- The increasing digitalization of the insurance business is going to have the biggest influence on changing fraudulent behavior.

- While data is seen as the enabler for AI, effectively harnessing it for fraud detection is viewed as a challenge.

Effective Anti-Fraud Techniques for Insurers

Over the past decades insurance companies have invested in various insurance fraud detection technologies. These technologies have evolved over the years from manual red flags; to reporting and data visualization; to automated business rules; to predictive analytics. Despite generating high positive rates in some cases, these techniques have proven to be effective to various degrees at spotting known fraud schemes. Traditional rules are useful to address known fraud patterns, but are less effective at addressing the sophisticated and evolving fraud patterns insurers are seeing today emerging from the increased use of digitalization. Staying ahead of the “fraud curve”
benefits both insurers and consumers. Such early detection remains one of the greatest potentials for AI.

Nearly every insurance company has undertaken a digital initiative. Online new business applications, mobile apps to submit claims and other self-service capabilities help insurers to improve their customers’ experience. These technological advances have also been a boon for fraudsters. Research shows organizations that have implemented a digital initiative have uncovered a significant increase in fraudulent activities. Survey respondents predict digitalization (56%) will have the biggest influence on changing fraud patterns, ahead of the economy (33%) and organized fraud (11%).
Question: What trend do you think is having the biggest influence on changing fraud patterns?

In this environment, property/casualty carriers report that technology plays an important role in detecting and combating insurance fraud. Research conducted by the Coalition Against Insurance Fraud in 2019 indicated 95 percent of insurers say that they are using some type of anti-fraud technology.1

A combination of techniques usually is required to identify opportunistic and organized fraud. Nearly 75 percent of respondents to the online survey believe that among relevant technology, AI will have the greatest impact on claims and fraud detection over the next five years.

AI Technologies and Techniques

Insurers are no strangers to AI. The technology already influences underwriting, marketing and product development. Insurers increasingly set premiums using complex algorithms that process massive amounts of data to predict future claims activity. Such activities, in the past have included “price optimization,” a practice now banned in many states. Because of its use in other operational areas, many insurers are finding broad support internally for adopting AI in fraud fighting.

Among the various AI technologies that have been deployed include:

- **Anomaly detection.** With anomaly detection, the user defines baselines for key performance indicators (KPIs) associated with tasks or events, then sets thresholds. When a threshold for a particular measure is exceeded, then the event is reported. Outliers or anomalies are used to identify existing, or new and previously unknown, fraud patterns.

- **Network analysis.** Organized fraud involving multiple linked claims and entities is pervasive and continues to expand. To address organized fraud

rings, insurers are looking to capitalize on emerging, highly sophisticated capabilities to analyze social networks and identify connections and patterns. Network link analysis has proven effective in identifying organized fraud activities by modeling relationships between entities in both the claims and new business acquisition processes. While link analysis is not new to fraud investigators, AI’s ability to analyze massive amounts of data and “connect the dots” takes such analysis to levels never before seen.

- **Natural Language Processing.** NLP is a branch of artificial intelligence that helps computers understand, interpret, and manipulate human language. NLP draws from many disciplines, including computer science and computational linguistics, in its pursuit to fill the gap between human communication and computer understanding.

- **Machine learning for scoring (neural networks, random forests, etc.).** This technology uses mathematical algorithms that can learn from data without relying on rules-based programming. With every iteration the algorithms become smarter and deliver more accurate results. Machine learning (ML) is split into two sections—supervised and unsupervised learning. Unsupervised ML is very effective in detecting suspicious activities when users don’t know what specific data may indicate fraud.

- **Speech recognition.** Sentiment analysis algorithms can be used during customer communications to analyze speech patterns and voice. Combined with spotting keywords identification corresponding to certain sentiments, speech recognition can provide strong indicators of potential fraudulent behavior that most humans would never be cognizant of during the conversation.

- **Image & vision analysis.** Image analysis allows the computer to determine if the subject of the photo is indeed the insured object. For example a broken television, flooded basement, cracked headlight or if it is something completely unrelated. In addition, image analysis can also verify that a photo has not been used in previous claims, downloaded from the internet or manipulated in various ways.
**Web crawling.** A new area of text mining focuses on the ability to analyze the huge amount of data available within the realm of social media platforms. Investigators are now searching publicly accessible Facebook, Twitter, SnapChat, Instagram, LinkedIn, Craigslist and other social media sites for evidence of non-meritorious claims. While this social media angle is rather advanced, some insurance companies are using software to effectively mine and analyze this unstructured text data in meaningful ways.

Yet, even with the great expansion of technology available to deploy in the fight against fraud, the room for growth is substantial both with current technologies and with those which will be developed in future years. On average, insurers are only receiving 15 percent of fraud referrals from their automated systems, according to a benchmarking survey of 40 property/casualty insurers conducted by the Coalition in 2019. While that percentage has not grown in recent years, the quality of referrals from technology has increased markedly, insurers say, thanks to advances in their systems. Improvements curtailing false positives or other inaccuracies benefits policyholders or claimants who are submitting legitimate claims and helps insurers by not wasting valuable staff time and resources on non-fraudulent claims.

**Challenges and Lack of Adoption of AI for Fraud Detection**

Artificial intelligence is disrupting nearly every step in the insurance value chain. While some insurance companies are investing heavily in AI, most insurers are moving slowly, unsure of how to deploy and use this technology. This study shows insurers are awaiting further development of legislative or regulatory provisions involving the use of AI before investing heavily in technologies which may be subsequently ruled improper. Others may be concerned about court decisions and jury verdicts addressing the use of technologies on claims where coverage is ultimately denied.

2. [https://www.insurancefraud.org/jifa/jul-2020/benchmarking-study-insurers-finding](https://www.insurancefraud.org/jifa/jul-2020/benchmarking-study-insurers-finding)
Question: What are your primary concerns with using AI? (select up to 3)

Survey participants were asked to name the top three concerns regarding the use of AI. The overwhelming concern was associated with data, with 52 percent of respondents indicating both data quality and insufficient data as their primary concern for the lack of adoption for AI. Not only is it true that the more data applied the more accurate the AI models, but also the philosophy of “garbage in, garbage out” applies. Interestingly, despite increased regulations pertaining to data protection, less than 15 percent saw data privacy as an inhibitor for AI.

Despite a lack of concern related to data privacy blocking AI adoption, other regulations are still of concern. The insurance industry is heavily regulated in most jurisdictions and many view AI as a “black box” application. Without transparency into how the machine-learning algorithms have been developed, regulators and other policymakers may be more apt to block or limit the carriers’ efforts to leverage these new applications. Lack of transparency and regulatory approval were cited as primary concern by 15 percent of the survey respondents.

Simply implementing AI to fight fraud could prove problematic if insurers do not fully understand the technology and techniques. Based on feedback
from interviews with leading P&C insurers it is essential to consider the following points when selecting software and vendors.

Lessons learned from these insurers include:

- It is important to understand AI, what it can do-- and just as importantly-- what it cannot do to detect fraud.

- Selecting software vendors and AI solutions primarily based on ease of implementation is not sufficient. One-size does not fit all. AI solutions must take into account an insurer’s book of business, risk tolerance and claims experience.

**Benefits of AI in Insurance Fraud Detection**

The adoption of AI for fraud detection in the insurance industry has been slow, however that is apparently about to change. Nearly half (48%) of the respondents indicate that their organization is likely to increase its investment in AI over the next 12 months.

One aspect that is driving that investment in AI is data. Data has always played a critical role in fraud detection. In the past, insurance companies have relied on traditional data, largely from human-driven claims and policy systems to identify suspicious activities. With digitization and other advances in technology, the insurance sector has access to significant amounts of new information. Unfortunately, traditional methods of fraud detection are not sophisticated enough to analyze all of this new data in a timely enough manner, nor with the same accuracy and depth of analysis. Many insurers have already made staff reductions in many areas, including SIU, leaving fewer humans to analyze the data necessary to identify the presence of fraud. By contrast, AI thrives on prompt and in-depth analysis of data, both structured and unstructured, and the more the better. According to one SIU director, “Big data allows AI to be effective and more accurate. As more data become available, AI will become even more useful in uncovering suspected fraud that previously was undetected.”
When asked “Besides claims and policy data, what additional data sources is your company using for fraud detection?” The survey identified social media data (78%), such as Facebook, Yelp and Vital as its go-to external data set. It is worth noting that most of this data did not exist 10 years ago. What we define as crucial data to analyze today will also change in coming years. Some existing data sources will no doubt disappear or become less relevant, only to be replaced by more new and innovative platforms.

There is a growing list of examples where insurers are using social media data to prove fraudulent activities. For example, disability claimants posting photos of them riding jet-skis, running marathons or climbing mountains. Video of a now former New York police officer fist-pumping while performing with his punk rock band, while on workers’ compensation for a shoulder and arm injury, has been a favorite example seen by many fraud-fighters.

**Question: Besides claims and policy data, what additional data sources is your company using for fraud detection?**

Other types of data that insurers are using include government and public data (67%), unstructured data like adjuster notes and police reports (63%) and video (40%). This was confirmed by a senior insurance executive who said “Insurers need to identify the specific types of internal and external data sources for an AI solution to detect suspicious activity. While the AI solution should be flexible for integrating a variety of different types of data.” A key advantage of AI is the ability to analyze huge amounts of data, especially unstructured data like images and scanned documents, at scale. For example, AI can examine a photo and then compare that image with millions of other photos in the insurers database to see if it has been used in any prior claims.

Insurance fraud comes in many shapes and sizes. When asked in what areas will AI have the greatest impact in the future for combating fraud, the most popular response was by far auto claims with over three-quarters (78%), with medical fraud (52%) and organized fraud (44%) rounding out the top three.
Question: In what areas do you think AI will have the greatest impact in combating fraud? (select up to 3)

Body shops billing insurers for fake windshield claims is a common auto insurance scam but discovering those claims in real-time, and at scale, is a major challenge. AI has the ability to identify these fraudulent claims by using anomaly detection to spot outliers on whether or not the body shop is charging considerably more than its peers for the same service.

Most insurers continue to focus on claims fraud, but fraudulent activities are prevalent through the entire insurance policy lifecycle, from the initial application process to claims and through to renewal. AI will have applicability in underwriting fraud, agency fraud and anti-money laundering. Savvy insurers will promote their use of AI to save policyholders from both fraud and the resulting higher premiums.

The goal of using AI in insurance fraud detection is to efficiently generate good referrals and make it easier for investigators to investigate suspect claims and transactions. “AI technology is not an alternative to employing investigators and claims analysts. It should be viewed as a tool to generate alerts for
potential fraudulent activity. Plus provide comprehensive reasoning why the claim was identified as suspicious to aid the investigation,” according to one SIU director. Fortunately, concerns about AI replacing humans and taking over the fraud detection and investigation process are unfounded. In fact, the common feedback from the interviews with the insurance executives is that AI is an enabler and seen as the next generation of fraud detection tools. Insurance companies still need humans and SIU teams to investigate the suspicious activities. Striking the right balance between “downsizing” and “rightsizing” will present challenges as the respective roles of humans and computers in the anti-fraud process evolve. This is also a topic that is being watched closely by many insurance regulators across the nation.

AI will not — and should not — replace human expertise when it comes to evaluating fraud. Despite an excellent track record, the algorithm won’t always get it right. This is, especially when dealing with either a new data source or an emerging fraud scheme. Or if the AI models have been based on a relatively
small dataset. Sometimes what looks like fraud may have a valid and benign explanation.

Public policy issues

“Artificial intelligence,” “big data” and “data privacy” are terms and practices that have, and will continue to, come under scrutiny by regulators, legislators, academics and consumer leaders in the U.S. While most of the focus in insurance is on underwriting and claims, fraud fighting efforts will also appropriately be subject to analysis and review. The goal and test will be to demonstrate fraud-fighters are using AI correctly and ethically to identify and fight fraud thereby benefiting insurance consumers. Failing to do so could result in negative impacts as restrictions are placed on obtaining and using data and technology systems.

In AI, the issues mostly focus on the potential for unfair discrimination, bias and privacy. Faulty algorithms obviously can lead to false positives, but so can well-written code. For example, in detection models, a positive hit could result when a claimant’s Internet searches were found to contain the words “fraud” or “arson” or similar terms. But those same terms are used frequently by researchers, academics and investigators themselves. Even the best AI can have difficulty determining the intent of internet searches.

More seriously, AI and big data can inadvertently discriminate unfairly against protected classes as well as against those in precarious socioeconomic situations, according to published studies. Insurers need to understand the potential for discrimination by their technology systems and ensure policies and procedures are in place to root out potential bias. The increasing use of artificial intelligence has raised the issue about model bias and fairness. Especially when associated with age, gender and most importantly in today’s environment, race. Recently the National Association of Insurance Commissioners (NAIC) has announced a major initiative to address race and insurance in America. Such considerations will no doubt look closely at systemic bias and practices across all aspects of the insurance spectrum.
AI models in and of themselves are not biased. According to an article by Harvard Business Review, AI can learn biases that skew outcomes if the database contains biased information or were built based on flawed practices. If the database is polluted with potentially biased variables like age, gender and race then it is important to remove or filter these variables from the model. However, even if these variables are not used, AI models could still be seen as biased because of how humans may interpret the results. For example, if a model is built to predict the next insurance CEO and it excludes age, gender or race from the data, it likely would still come to the conclusion that the next CEO will be male, over 50 years old and white. This is because the historical data is skewed to these results. While the times are starting to change with more diversity in today’s insurance industry leadership, far more progress is needed so when these models are run in future years the results will be different.

Insurance regulators are grappling with understanding AI and its implications of its use on consumers. The NAIC created a working group in 2019 to study the impact on consumer protection and privacy; marketplace dynamics; and the state-based insurance regulatory framework. The mission of this panel was to develop guidelines for state regulation of policies governing insurer use of AI. The final guidelines, which were recently adopted unanimously by NAIC members, call for insurers to be fair and ethical, accountable, transparent and ensure their AI systems are secure, safe and robust. “AI systems must not be designed to harm or deceive people and should be implemented in a manner that minimizes negative outcomes,” according to the NAIC guidelines.

Now finalized, the guidelines likely will be the basis for new state regulations governing insurer use of AI technology.

When used properly, consumers should have less risk of harm and insurer SIUs have less at stake than other areas of their companies when it comes to negatively affecting policyholders, applicants and claimants. The reason is no conclusion of fraud — including claim denial — should ever be based solely on a positive hit from a technology system.
Verification via professional investigative techniques by analysts and investigators serves as a vital consumer safety backstop against false positives. If anything, systems that are not finely tuned will produce more false negatives, allowing fraudulent activity to go unchecked.

Still, SIUs and their technology vendors need to ensure their technology systems are not unfairly scrutinizing claims and applicants because of race, gender, geographic location or any other potentially improper factors.

**Conclusion**

Fraud detection is an ever changing and growing problem, especially considering the COVID-19 pandemic and subsequent impact on the economy. Fraudsters have a long track record of developing new approaches to evade detection or operate in ways that did not exist just a few years or even months ago.

Savvy fraudsters, especially those in organized rings, are using technology to detect weaknesses in payment systems or other insurance loopholes. And don't think for a minute fraudsters themselves may well be employing AI to find ways to commit fraud. Insurers and others in the fraud-fighting community — including state fraud bureaus — should have a broad range of the best tools, including AI, to counter and be ahead in the fight against insurance crime.

The use of AI as an effective anti-fraud tool will become even more important as more data becomes available to fraud fighters, making machine learning that much more accurate and able to adapt as quickly as the fraudster’s changing tactics.

For the future, it will be interesting to see whether insurers use this technology not only to better detect fraud, but to prevent it. If the technology can predict fraud spikes, insurers will be able to allocate resources to those areas and even employ techniques to deter fraudulent activity, such as a greater anti-fraud presence and public awareness campaigns.
Appendix

Survey Questions

Q1: Is your company currently using AI for fraud detection?
   - Yes
   - No
   - Don’t know

Q2: As a result of the COVID-19 pandemic, do you foresee your organization
   - Increasing your use of AI
   - Delaying use of AI
   - Having no impact

Q3: How does the prospect of using AI for fraud detection make you feel?
   (on a scale of 1 to 5 with 1- as concerned to 5 as excited)

Q4: What are your primary concerns with using AI? (Select up to 3.)
   - Model bias
   - Lack of transparency / black box
   - Replacement of human resources
   - Lack of data science resources
   - Regulator’s approval
   - Data privacy
   - Data quality
   - Insufficient data
   - Lack of adoption

Q5: Will your company's investment in AI likely increase in the next 12 months?
   - Yes
   - No
   - Don’t know
Q6: How do you view your company’s fraud detection process in comparison to your competitors? (Using a scale with 1 being "lagging" to 5 being an "industry leader.")

Q7: In what areas do you think AI will have the greatest impact in combating fraud? (Select up to 3.)

- Auto claims
- Property claims
- Medical fraud
- Commercial claims (workers comp, liability)
- Organized/professional fraud
- Soft or opportunistic fraud
- Application or underwriting fraud
- Agency fraud
- Anti-money laundering

Q8: Besides claims and policy data, what additional data sources is your company using for fraud detection? (Check all that apply.)

- Government and public data
- Social media (Facebook, Yelp, BBB, Vitals etc.)
- Photos and aerial imagery
- Video
- Unstructured data (adjuster notes, emails, etc.)
- Other

Q9: What trend do you think is having the biggest influence on changing fraud patterns?

- Digitization (online, mobile apps etc.)
- Organized fraud
- Economy

Q10: What technology do you see having the most impact on claims and fraud detection in the next 5 years?

- AI / machine learning
- IoT (telematics, drones, FitBits, etc.)
- Insurance company mobile apps
Q11: What is your company's primary business?
- Auto
- Commercial
- Disability
- Homeowners
- Life
- Workers compensation

Q12: Which of the following best describes your job function?
- Senior management
- SIU director/manager
- Other

Additional comments and feedback from the interview with leading property/casualty insurers on considerations to deploying AI technology

- Consider if the AI solution will be implemented and maintained in-house or by a third-party host. That decision impacts company resources, implementation timeline, project costs, and ongoing expenses.

- Does the AI solution build on existing anti-fraud technology tools or processes already in use? Is it entirely new or a replacement? Those answers will drive the project scope, features, and enhancements of the solution.

- What are AI solution software features and functions out-of-the-box, and do they meet current and future business needs? Can the AI solution be reasonably customized or configured to an insurer's specific needs.

- Is the AI solution holistic by the use of multiple modeling methodologies and algorithms, and what does the feedback loop look like that will drive the model retraining and machine learning process?
• The right AI solution on the frontend for scoring claims, providing some level of reasoning and alerting adjusters, should require minimal training for claims staff and would typically be handled internally. On the backend, the tools that typically the SIU interfaces with through a (UI) user interface are end-user training and vendor-provided, and the internal workflows and business processes are company-specific and typically in-house training.

• Develop a partner relationship with the selected technology vendor and commit to a high level of collaboration to monitor models and refine outcomes.

• Early adopters in the insurance industry made their share of mistakes in trying to use AI in detecting fraud activity. Among the errors:

  o Failure to define and maintain project objectives and scope. Unrealistic expectations around the AI solution's effectiveness and the expected immediate return on investment early in the process post-implementation.

  o Relying on technology while ill-prepared and not having the experience or resources in place to screen and properly investigate AI alerts and claims.

  o Not aligning investigative resources and capabilities with AI output in such a way as to appropriately and accurately measure the output. The AI can be accurate but if the investigative technical abilities are lacking, it gives a false indication that the AI is lacking as well, which may not be the case.
Acknowledgements

This study was conducted by the Coalition Against Insurance Fraud with technical and funding assistance from Shift Technology, a leading company in the field of fraud analytics.

Technical review also was provided by the Coalition’s Research Committee, which includes:

- David Rioux, Erie Insurance
- Steve Friedman, Liberty Mutual
- Steve Piper, CNA
- Jack Dever, American Family
- Steve Jarrett, Westfield Group
- Tim Hopper, Sentry Insurance
- Joe Theobald, Citizens Insurance
About The Coalition

The Coalition Against Insurance Fraud is America’s only anti-fraud alliance speaking for consumers, insurance companies, government agencies and others. Through its unique work, the Coalition empowers consumers to fight back, helps fraud fighters better detect this crime and deters more people from committing fraud. The Coalition supports this mission with a large and continually expanding armory of practical tools: Information, research & data, services and insight as a leading voice of the anti-fraud community.

For additional information on the Coalition Against Insurance Fraud contact us at 202-393-7330 or info@insurancefraud.org

About Shift Technology

Shift Technology, founded in 2014, has developed an AI-native, purpose-built fraud solution for the global insurance industry, deployed via a SaaS model. Based in Paris, Shift Technology now has a footprint of over 70 insurer and anti-fraud customers in Europe, North America, and Asia. With the recently announced funding round of $60 million, the company has raised a total of $100 million in capital and has rapidly matured both in terms of business organization and solution capabilities. The foundational strength of the company is its world-class data science capabilities and extensive insurance claims experience. Shift’s FORCE solution is being used for a wide variety of fraud scenarios and is applicable across multiple insurance lines of business. In addition, insurers are discovering that the insights gained from the analysis of new data sources enable increased claims automation across the value chain.