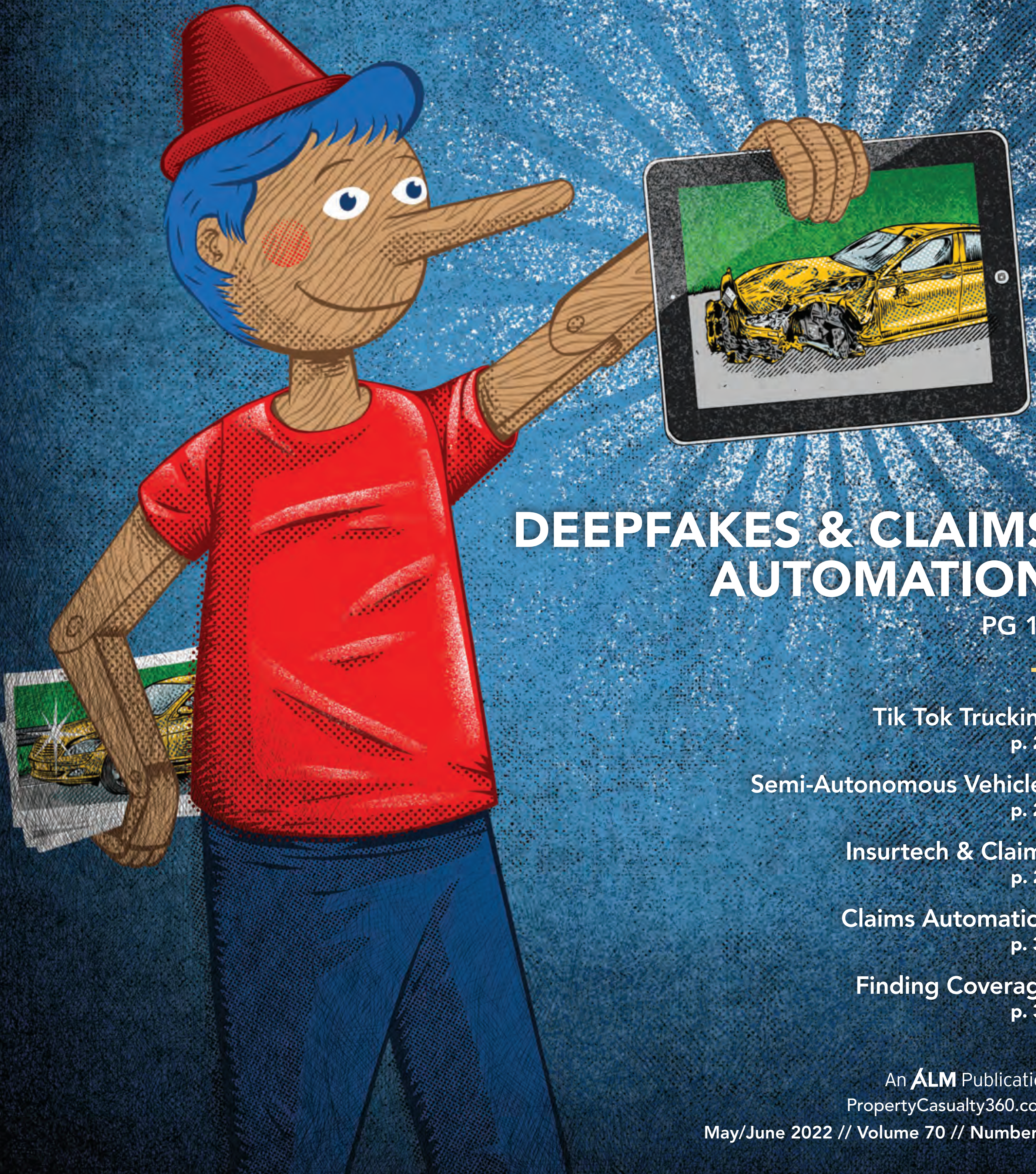
NU Claims

COVERING THE BUSINESS OF LOSS



DEEPFAKES & CLAIMS AUTOMATION

PG 16

+

Tik Tok Trucking
p. 20

Semi-Autonomous Vehicles
p. 24

Insurtech & Claims
p. 27

Claims Automation
p. 30

Finding Coverage
p. 34

An ALM Publication
PropertyCasualty360.com
May/June 2022 // Volume 70 // Number 3

HOW DEEPFAKES THREATEN CLAIMS AUTOMATION

By Nicos Vekiarides | Illustration by Boris Séméniako

IF YOU READ THE SEPTEMBER/OCTOBER 2021 CLAIMS Magazine article entitled *Deepfakes: An Insurance Industry Threat,* you are familiar with the threat that deepfakes and synthetic media, in the form of photos and videos, pose for the insurance industry. From exaggerated claims to the creation of fake assets, AI-generated images and videos call for protective action by insurers to defend against this burgeoning form of fraud.

THE RELENTLESS ASSAULT OF FAKE MEDIA

The past several months have confirmed that deepfakes are much more than a passing fad. From fake images and videos used as war propaganda in Ukraine, synthetic creation of movie actors, cryptocurrency scams, to document and identification fraud, the cases where deepfakes establish false narratives and circumstances have steadily increased. Once limited to a social media novelty, deepfake fraud has emerged as a formidable threat across many industries. Its potential to impact the insurance industry, which already suffers from over $80B in annual fraud in the U.S., is immense.

In response to this threat, new and developing industry standards, such as C2PA and the Content Authenticity Initiative, have led to the release of proposed specifications for protecting the authenticity of photos. Other solutions, such as blockchain-based tamper-proofing and AI analysis, have continued to mature to better meet the scale required by claims processing, offering more options to firms looking to take action. In light of these potential mitigation strategies and solutions, how is the insurance industry reacting?

WrightStudio/Adobe Stock

AWARENESS AND CONCERN AMONG INSURANCE PROFESSIONALS

The problem of altered digital media is not entirely new to insurance. While photo editors began to proliferate many years ago, deepfakes have complicated the problem exponentially by making it harder to detect digital media fraud.

In a recent survey of insurance professionals by Attestiv, over 80% of respondents indicated concern for altered or tampered digital media used for insurance transactions, such as claims. This is a clear acknowledgment of the threat and the fraudulent losses that can result. In fact, altered photos that falsely inflate claims were the top concern among the various types of media-related fraud. But when do these organizations plan to take steps to solve this problem?

When asked about their timelines for deploying digital photo and media validation, 22% responded they already have a system in place, while another 11% indicated they would have a system within the next year. Putting those together, a total of 33% of organizations indicated having or being close to having a validation solution, leaving 67% of organizations relatively exposed.

KEEPING UP WITH TOUCHLESS AUTOMATION

While there is some movement from insurance organizations to close the gap of deepfake fraud, the pace of touchless automation, in the form of self-service transactions and straight-through processing (STP), has been far faster and a bit more furious. No doubt, COVID may have aided the transition to self-service transactions, as it was a natural fit for claims reporting during lockdowns. At the same time, this mostly welcome digital transformation increases dependency on customer-supplied photos for settling claims.

In contrast to responses on digital media validation strategies, over 43% of survey respondents indicated having self-service claims available now, while another 7% indicated availability within the next year. Likewise, 49% of respondents indicated having STP claims systems now, while another 7% indicated availability within the next year.

The deeper implication of this relatively torrid pace of automation is that with customer-provided photos and virtually no human interaction on the claim processing side, the risk of fraud from altered, manipulated or synthetic photos significantly increases. If we focus solely on the present, 49% of respondents using STP claims and only 22% of respondents using a photo and media validation system leaves a large gap of exposure. Ultimately, who is minding the photos and what can be done about the inaction gap?

INDUSTRY EXPERTS WEIGH IN

Experts in claims processing, insurtech and the industry tend to agree that the risk of image fraud has been small to date, perhaps leading to a false sense of security. However, the problem is poised to increase over time.

"In general, from the beginning of COVID in 2020 through 2021, the industry saw an increase in user-submitted photos to streamline workflows," said Ernie Bray, CEO of Auto Claims Direct (ACD). "I think now many insurers are starting to become receptive to embracing photo verification, and if the true mission is to accelerate claims processing, photo validation will be at the forefront."

Others, like Michael Lewis, CEO of claim technology, suggest a very proactive approach to building out counter-fraud, saying, "Customer self-serve and digital counter-fraud are two sides of the same coin. You shouldn't be introducing the former without first having implemented the latter."

Going a step further, another approach is to build up a counter-fraud approach prior to automation. Laura Drabik, chief evangelist at Guidewire Software, suggests, "AI technology of fake or altered media can augment the human – today. Rather than rely solely upon the adjuster, technology can detect subtleties and patterns that the human eye cannot."

For those choosing inaction, on the other hand, Alan Pelz-Sharpe, founder of analyst firm Deep Analysis warns, "In a world of simple to access and use tools to doctor images, it's all too easy to defraud. The risk and regularity of this kind of fraud is likely low today, but it will certainly increase substantially over the coming years."

So while all may be quiet for the moment, the cost of inaction may be high. "In all likelihood, few if any insurance firms have addressed this growing concern. Yet it should be a priority for them as once this takes off — and it will, and it will be hard to stop," said Pelz-Sharpe.

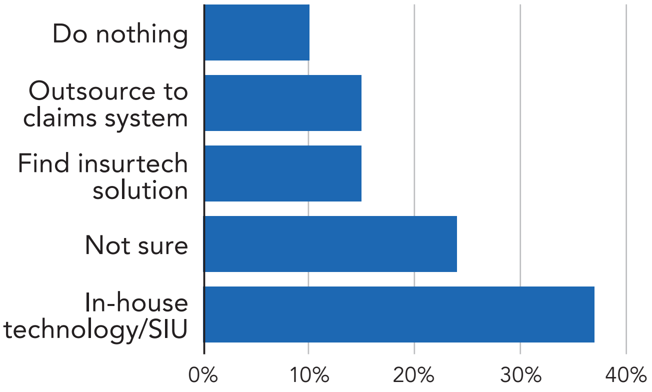
WHERE ARE THE SOLUTIONS?

Those hoping to see the industry rapidly huddle around a common solution for the problem may be disappointed. In fact, survey respondents indicated a huge variance as to how organizations source and stand up digital photo and media validation solutions.

Unsurprisingly, 24% of insurance respondents were not sure of their approach to a solution, indicating nascent stages of planning or perhaps avoidance of the looming issue. Thirty-six percent said they would either rely on in-house technology or their SIU to solve the problem. That is a relatively high percentage who would prefer to build the expertise in-house or lean on groups already being heavily utilized. While 15% would consider an insurtech solution to solve the problem, nearly another 15% would prefer to outsource the solution to claims providers or systems. Finally, 10% are content doing nothing about the problem.

Bray advises, "Having an AI-powered anomaly detection built into a claims process is one more step to stopping fraud and increasing accurate claim handling. Without any ability to check the authenticity of photos, damages could be exaggerated, and carriers will be ultimately paying for losses that are either inflated or entirely false."

FIGURE 1
HOW ORGANIZATIONS SOURCE AND STAND UP DIGITAL PHOTO AND MEDIA VALIDATION SOLUTIONS



With such a high percentage sticking to the status quo, unsure or ignoring the problem, Lewis reminds, "Much has been said about the importance of keeping an adjuster in the loop to prevent fraud, but no adjuster can be trained to detect image or document tampering that is invisible to the naked eye."

WHAT DOES THE FUTURE HOLD?

While fraud has always been a well-known challenge in insurance, the pace of claims automation is far exceeding the pace of automated fraud prevention, opening new risks and perhaps new opportunities. Some insurance companies may be willing to risk fraud vulnerabilities in return for cost savings elsewhere and an improved customer experience. Others may want to take a safer, more controlled approach, ensuring the development of fraud technologies keeps pace with claims automation to ensure the business does not experience unforeseen loss increases.

"It really comes down to insurers realizing the true ROI on photo authenticity. The cost to implement a solution to analyze the validity of photos can pay for itself many times over with one or two claims," said Bray.

Whether solutions to combat deepfakes and synthetic media are embraced, the past couple of years have shown that touchless claims (and underwriting) transactions are here to stay, and how digital media can be compromised has become more elaborate. As a result, proactively taking steps to implement automated fraud prevention technology is quickly becoming an important consideration for protecting the business metrics that matter most.

As Lewis concisely points out, "Running anti-virus on incoming attachments is non-negotiable. Shouldn't the same apply to running counter-fraud checks on every image and document?"

The risk of not adopting counter-fraud may be significant. As Drabik points out, "Ultimately, this will drive up the price of insurance for everyone, including the majority of people and families that don't commit fraud."

So what will it take to make insurers accelerate their media fraud prevention plans? "In reality, there will be some major success by organizations and individuals in defrauding insurance firms in the future," said Pelz-Sharpe. "Unfortunately, it will likely take a major case to come to light and gain some embarrassing headlines before firms take action to mitigate the risk."

Ultimately, it is hard to speculate about the adoption of deepfakes, synthetic media and associated countermeasures in industries such as insurance and whether fraudsters will see the technology as an opportunity to victimize companies who have not taken measures. What is certain is that the next few years will become a clear indicator of whether those organizations taking proactive measures today have invested wisely.

Nicos Vekiarides (nicos@attestiv.com) is the chief executive officer & co-founder of Attestiv. As a CEO & entrepreneur, he has spent the past 20+ years in enterprise IT and cloud, bringing innovative technologies to market.