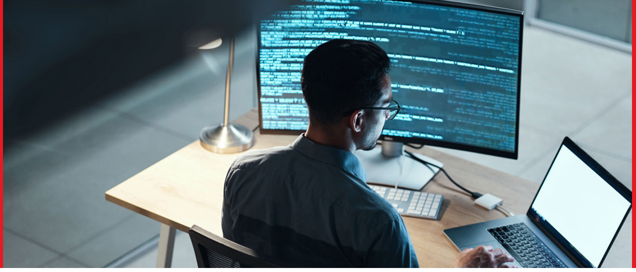

Artificial Intelligence and Insurance Fraud: Four Dangers and Four Opportunities

IN BRIEF

Insurers should monitor the latest AI-assisted hoaxes and learn more about how to harness the power of AI to uncover potential fraud throughout the insurance pipeline.

Neil Parkin
Head of Business Development,
RGA South Africa

Impersonation is at the heart of insurance fraud – for example, fake physicians submitting fake medical records to support fake claims. Someone – or something – needs to supply the fake content, and generative artificial intelligence (AI) is more than available to fill the role. AI is fast becoming a criminal's best friend.

Fraudsters once needed extensive technical skills to set up and execute their schemes. Today, the average criminal only needs to apply one of many easy-to-use and accessible AI tools. These provide sophisticated capabilities in writing, coding, and image generation and manipulation. Taken together, they create the perfect storm of criminal innovation and criminal opportunity.

The intelligence is artificial, but the crimes are real

Because they are trained on large language models, generative AI tools like ChatGPT are skilled at mimicking human speech and writing. Users feel like they are talking to real people, but AI-based chatbots also make all-too-human mistakes. Attorneys have learned the hard way never to rely on chatbots for legal research. In one recent episode, ChatGPT "hallucinated" cases with realistic-seeming, but false case citations, resulting in disciplinary action for one less-than-careful attorney. In another instance, a New Zealand grocery store created a bot to generate tasty recipes from submitted lists of ingredients. The same bot made news when it recommended an "aromatic water mix" based on a list of deadly household chemicals.

AI may occasionally produce nonsensical results, but in the hands of a skilled criminal, chatbots can create vivid, immersive simulations of people and even manufacture false medical evidence.

- **Voice cloning:** One method people can use to verify the source of a suspicious email or document is to call a listed phone number and speak directly to the sender. If the voice on the other end of the line sounds familiar and makes sense, it's a legitimate inquiry, right? Not if an AI product has used hacked recordings of the person to clone his or her voice.

  Scammers can sample a surprisingly rich and accessible audio archive of social media posts, video, and voice memos to build a library of speech – and it doesn't take much. Researchers at McAfee Labs needed just three seconds of audio to produce a clone of a human voice with an 85% match to the original recording. About a minute of audio can push accuracy rates up to 95%, close enough to fool employers, family members, and insurance investigators.

- **Deepfake photographs and video:** Deepfakes are synthetic media, digitally manipulated to convincingly replace one person's likeness with that of another. One image that circulated on social media showed former U.S. President Donald Trump browsing a rack of orange prison jumpsuits. Another image depicted the former president tussling with police on the street. Both photos look hyper-realistic, but they were completely fabricated using AI tools. AI video systems are also available, empowering criminals to manipulate existing video footage to create false videos. It is even possible for criminals to fake video calls on Skype or Zoom, stealing a person's image and identity to advance their scams.

  Insurance executives or staff could be victims of these schemes. For example, fraudsters have created fake social media accounts in the name and image of actual banking professionals. These accounts show those individuals endorsing cryptocurrencies or extending false loan offers.

- **Medical evidence:** Criminals can use AI imaging tools to create convincing x-rays or CT scans, and then submit this fake medical evidence to insurers. For example, Bing's image generator can be prompted to create an x-ray of a fractured bone. Today, medical professionals could spot most fakes. However, to produce highly realistic images, AI systems are being trained on a vast store of radiology data. As AI image generators mature and produce more sophisticated images, these types of fraud will become more prevalent and more successful.

- **Professional documents:** Email scams and phishing attempts sometimes reveal their true nature through garbled language, misspellings, and other errors. These mistakes are often the consequence of fraudsters with limited language skills targeting potential victims in another country. AI chatbots have proven to be the perfect remedy. Criminals can run their phishing communications through ChatGPT to clean up spelling and grammar and produce a far more convincing message. AI bots can also translate messages into any language, allowing criminals to expand the range of potential victims.

  As one example, I was able to use AI tools to draft a letter from a fake physician excusing myself from work for six weeks due to an accident. My initial prompt – "Write a doctor's note excusing Neil Parkin from work" – provoked this response from ChatGPT: "As an AI model, I cannot write official documents, such as a doctor's sick note, because it requires personal information and medical expertise." At last, here is a helpful guardrail on AI. But when I adjusted my prompt and requested a template for sick notes, ChatGPT happily complied. I then used an AI image tool to generate a fake logo for the physician's office. The final product was a professionally written – and completely false – sick note produced on a doctor's letterhead.

> AI technologies contribute to the "professionalization" of criminal scams. Deceptions look better, sound better, and are more convincing to individual targets.

The positive potential of AI

Insurers need to be on alert for AI-assisted scams. But the industry is also looking to AI tools to flag deceptive claims and reveal fraud attempts. Not all these capabilities may be available yet, but as criminals expand their use of AI, the insurance industry should likewise explore its ability to root out AI-assisted fraud.

- **Risk profiling:** AI can enhance risk assessment and provide more nuanced details about insurance applicants. Artificial intelligence could also identify itself, flagging applications that may have been created using AI tools.

  Insurance is just one of many industries with a vested interest in detecting AI-assisted content. The academic world has been keen to identify AI-written work submitted by students. Some plagiarism software makers, like the creator of Turnitin, are now focusing on AI detection. Even the creators of ChatGPT, OpenAI, have hired a data scientist to develop a possible "watermark" for ChatGPT responses, which will take the form of a secret set of words and punctuation. To an outsider, the text looks normal, but those with the right "key" can detect the watermark.

- **Underwriting:** AI has the potential to automate many steps in the underwriting process. Actuaries are already testing AI capabilities for mortality calculations, coding, and other uses. AI could also examine data, such as the time an applicant needed to complete an online form, and flag fraudulent applicants who answered questions more quickly than an actual human could. AI tools are only as powerful as the data used to train them, so in these instances, it will be essential for insurers to track their own data to feed any models.
- **Claims:** An AI tool trained on fraudulent claims could become skilled at flagging them. It could also detect the types of AI-created scams detailed above, like doctored photos and videos, audio recordings, and AI-generated narratives. Such tools could also expose fraudulent claim patterns, such as the use of repeated mobile numbers or physician names.
- **Fraud monitoring:** Lastly, if fed historical data about fraudulent claim attempts, AI tools could be incorporated throughout the insurance pipeline to pinpoint fraud "hot spots," trends, and patterns.

Again, many of these AI-detecting capabilities may be years off, but criminals are using AI tools now to defraud individuals and companies out of millions of dollars globally. Our industry must stay informed and vigilant about the latest AI developments so we can protect our business interests, our customers, and our own reputations.

At RGA, we are eager to engage with clients to better understand and tackle the industry's most pressing challenges together. Contact us to discuss and learn more about the RGA capabilities, resources, and solutions.