

Hey! What's New? 2025-58

How CPAs Can Combat the Rising Threat of Deepfake Fraud

Andrew Kenney writes in an article in the latest issue of the *Journal of Accountancy* that, last year, Deloitte polled more than 1,000 executives on their experiences with deepfake attacks. Nearly 26% of the respondents said their organization had experienced one or two in the previous 12 months. And more than half of the respondents (51.6%) expected the number and size of deepfake fraud attacks targeting their organizations to increase over the subsequent 12 months.

"We hear about more and more of these on a regular, everyday basis," Jonathan T. Marks, CPA/CFF/CITP, CGMA, a partner in BDO's Forensic Accounting & Regulatory Compliance practice, told Kenney. Finance and banking, he said, are key targets because of their access to money and data.

"If people are not paying attention to this, it might be too late when an incident happens — especially with the speed at which information can get moved, funds can get transferred," said Satish Lalchand, a principal in Deloitte Transactions and Business Analytics LLP who specializes in fraud detection and AI strategy.

But, says Kenney, finance professionals can take action to mitigate the deepfake-fraud risk. "The Deloitte poll, for example, highlighted what respondents said they have done."

Can you spot a deepfake?, he asks. "It's sometimes possible to identify a deepfake by observing it closely. AI-generated images may have incongruities, such as a person with too many fingers or a nonsensical layout for a building. Synthetic video or audio of a person may simply feel off in a way that's hard to pinpoint."

"It's lighting, it's cadence, it's these certain things" that can betray an imposter, Marks said.

Kenney points out that "deepfakes are digital imitations of images, videos, documents, and voices fraudsters create with generative AI. They gained widespread public attention through head-spinning viral videos — like an eerily accurate digital clone of Tom Cruise, complete with convincing facial expressions and body language."

And deepfakes are advancing just as fast as AI, he adds. "The technology is becoming more widespread and easier to deploy. The advances can make the tells that something is a deepfake more subtle, and scammers can mask flaws by transmitting the video in lower resolution or by inserting digital noise and compression artifacts (distortions that can appear when video is compressed)."

The increasing power and accessibility of deepfake technology also means that attackers can pursue a wider range of victims, Kenney warns. "Previously, a convincing fake might have been feasible only if the subject person was featured in a large amount of audio and video recordings, but experts say the fakes now can be generated with far less source material. That could make it easier to target executives at smaller companies, even if there isn't much video or audio publicly available."

Deloitte's Center for Financial Services estimated that AI-generated fraud will reach \$40 billion in damages in the United States by 2027, a 32% annual rate of increase from \$12.3 billion in 2023.

"Gen AI tools have greatly reduced the resources required to produce high-quality synthetic content," FinCEN reported in its November alert.

For example, says Kenney, in March 2024, OpenAI, the company that developed ChatGPT, reported that its voice engine technology could generate "natural-sounding speech that closely resembles the original speaker" with just a 15-second sample.

He notes that "OpenAI acknowledged the potential abuse of the technology while also highlighting legal and technological guardrails it had put in place. But generative AI advances aren't just coming from tech giants anymore. As the open-source model DeepSeek has shown, small outfits can create advanced generative AI models. In other words, you won't catch every deepfake simply by looking for glitches. But other techniques may still help."

Kenney says that Clay Kniepmann, CPA/CFF/ABV, a forensic, valuation, and litigation principal at Anders CPAs + Advisors, advises keeping an eye out for odd behavior, such as a potential impersonator's lack of knowledge about the real person. "It's knowing who you work with," Kniepmann said. "Know who that approver is, what their personality is like."

More broadly, he says, "the most reliable defense may be to stay aware of the more universal signs of fraud — unusual and unexpected requests, false impressions of urgency and stories that don't stand up to scrutiny."

Learn a whole lot more at [How CPAs can combat the rising threat of deepfake fraud](#).