By: **Kevin M. LaCroix**

The D&O Diary

A Periodic Journal Containing Items of Interest From the World of Directors & Officers Liability, With Occasional Commentary

The Growing Threat of AI Deepfake Attacks

By Kevin LaCroix on August 19, 2025

A new wave of AI-powered scams is targeting companies by impersonating their most trusted leaders – the CEO, the CFO, and other senior executives. Cybercriminals are now using generative AI tools to create hyper-realistic video and audio deepfakes of company executives to trick lower-level employees into handing over millions of dollars in cash, critical data, and other business assets. While these kinds of scams aren't necessarily new, AI language and image models are making the scams increasingly effective and more prevalent, according to a recent *Wall Street Journal* article. The August 18, 2025, article, entitled "AI Drives Rise in CEO Impersonator Scams," can be found **here**.

The typical deep fake scam starts with a phone call to a lower-level employee with privileged access to a company's inner operations, from a fake CEO or other executive with an urgent request. The initial call is then followed by a one-on-one virtual meeting with a convincing video of the official, giving the worker specific instructions for wiring emergency funds, transmitting business data, or simply luring the worked to click on an emailed link with malicious code.

What makes these scams so pernicious is that the deepfake images or audio track are so effective. The automated image is designed to respond to questions or comments in real time, mimicking a natural conversational manner, including a recognizable voice or speech pattern, as well as familiar body movement or facial expressions.

The faked executives often are public figures, meaning that scammers are able to access troves of material – media interviews, promotional videos, webinars, earnings calls – the scammers can use to teach the AI models to learn someone's voice pattern, tone, and facial expressions.

Once trained, the scammers can use the AI tools to generate new clips that look and sound like the faked person.

According to the *Journal* article, there were more than 105,000 deepfake attacks reported last year. These figures may actually understate the problem as many organizations do not disclose the attacks to avoid reputational damage.

The losses from these kinds of scams are massive. The *Journal* article reported that AI-generated CEO and other executive impersonations exceeded over $200 million just in the first quarter of 2025. Nor is the harm from these attacks limited just to financial loss. The harm can also include reputational harm, operational disruption, and even legal exposure, if the attack results in the compromise of customer or employee data.

The problem may be getting worse. The U.S. Treasury's Financial Crimes Enforcement Network recently warned about an upswing in deepfake scams targeting banks, insurers, mortgage brokers, and casino operators. In July, at a Federal Reserve event, OpenAI CEO Sam Altman said he feared an upcoming "fraud crisis," triggered by the ability of AI to impersonate other people. (At least we THINK it was Sam Altman who made this statement...)

The problem is becoming so pervasive that we are now seeing the emergence of cybersecurity startups that specialize in deepfake detection. Many of these startups are seeking to advance AI-based tools, on a "it takes a thief to catch a thief" type model. However, according to industry experts quoted in the *Journal* article, technology tools alone may not be sufficient to stop or prevent the scams; "rigorous verification, staff training, and technical measures are all vital to defense." The bottom line is that voice and video impersonations are no longer merely a futuristic concept, but a present-day cybersecurity threat.

The pervasiveness of the deepfake problem has also caught the attention of legislators. At least **47 states have enacted some form of deepfake regulatory legislation**, though much of it is not really intended to address the kind of deepfake attack described in this post. Of the laws enacted so far this year, the three most common topics were bills addressing sexually explicit deepfakes (42 bills), bills dealing with political communications (8), and bills creating regulations on tech entities related to deepfakes (9).

Cyber liability insurance is evolving to address these new threats. Cyber insurance typically covers data breaches, ransom attacks, and social engineering fraud. Some policies now include endorsements for synthetic media and deepfake-related fraud. One thing to watch out for, though, is the possibility of AI-related exclusions. While this is not something that I am currently

seeing, the Hunton Andrews Kurth law firm **published a memo** earlier this year in which the firm noted what it called the "continued proliferation" of AI exclusions, including exclusions for loss arising from or caused by AI-generated content.

A.M. Best Podcast Interview: Some of you may be interested to know that I recently recorded a podcast interview with A.M. Best. Among other things, in the interview I discuss the history of *The D&O Diary*, and some of the lessons I have learned in writing the blog for nearly 20 years. You can find the podcast **here**.
