Press Coverage | July 16, 2026

AI Deepfakes Are Testing HR's Ability to Spot Fake Evidence

RELATED PROFESSIONALS

Tracey E. Diamond

Tracey E. Diamond, a partner in Troutman Pepper Locke's Labor + Employment Practice Group, was quoted in the July 16, 2026, *HRD America* article, "AI Deepfakes Are Testing HR's Ability to Spot Fake Evidence."

> Fabricated stories are nothing new in workplace investigations. But AI and deepfake technology are giving employees a more convincing way to back them up, according to Tracey Diamond, a labor and employment partner at Troutman Pepper Locke in Philadelphia.
>
> "It's sort of like a continuation of the old version of employees lying. They're just creating evidence to further their lies," Diamond said.
>
> "We're not seeing it a lot yet, but I do think that the possibilities are becoming more real because AI is getting more and more accurate. And the ability to create falsified documents, falsified time records, falsified pictures, it's just becoming harder to detect."
>
> Diamond has already encountered the problem firsthand. "I did have a situation with a workplace investigation not that long ago where there were falsified communications made," she said. "I don't know whether the person used AI to create that, but he'd used something."
>
> …
>
> Deepfakes create a two-sided problem for workplace investigations. Fabricated evidence can be submitted to support a false complaint, while employees accused of genuine misconduct can claim authentic evidence was manipulated. Either way, Diamond said the answer lies in old-fashioned investigative rigor.
>
> "They should follow proper investigatory techniques in terms of seeing what they could find to corroborate the story," she said. "For example, if someone is saying that an employee sent them a harassing text message, checking the employee's phone as well as the alleged harasser's phone to see if the messages are on both phones, checking the deleted files, performing forensics. Do the best they can to corroborate the story."
>
> When the stakes are high, she recommends bringing in outside help.
>
> "If it's an investigation that involves potential termination or a high-level situation that could put the company at risk, we recommend that they use outside experts to make sure they're getting it right," Diamond said.
>
> "The employer has an obligation to perform a prompt and thorough investigation and take action if they reasonably believe that a violation of their policies or, more importantly, a violation of a law took place," she said. "So if an employer ultimately gets it wrong, but after they conducted a thorough investigation and it was reasonable for them to reach that conclusion because the technology was that good, then that should protect them."
>
> …
>
> Diamond sees fabrication spreading well beyond investigations. She pointed to reporting on candidates using AI to fake skills in job interviews, a trend that echoes a problem one cybersecurity researcher demonstrated firsthand by using deepfake video to pose as a fictional candidate and getting hired.
>
> "We're seeing it creep into a lot of different areas of the hiring-to-firing life cycle," she said. "The limit is the cleverness of the workers."

©2026 Troutman Pepper Locke

Some visual tells still exist, at least for now. “When it’s a photo, sometimes you’ll see it looks like the person’s not standing exactly on the ground, or a piece of their body gets disappeared,” Diamond said. “But that is getting harder and harder to detect as the technology gets better.”

Her bigger concern is what the technology does to trust itself.

“It’s hard to be able to in good faith rely on what you’re seeing with your own two eyes if there’s a chance that it’s being faked,” she said.

…

Diamond doesn’t believe deepfakes require a standalone policy, but they should be addressed explicitly within an employer’s broader AI policy.

“While you’d think it goes without saying that AI should only be used to tell the truth, maybe it warrants saying that in a written policy,” she said.

Training should follow the same logic. “I do think that comprehensive AI training, including the concerns about deepfake technology, should be part of all employers’ training programs for sure now.”

She also urged HR leaders to build closer ties with their technology teams. “CHROs and other HR leaders should be working with their tech departments so that they’re aware of the capabilities of the technology, both for nefarious purposes and for good purposes.”

Beyond fraud and false complaints, Diamond flagged another risk on the horizon. Deepfakes can be weaponized against coworkers directly, using someone’s photo or likeness to damage their reputation or make them appear to have done something they didn’t.

“It’s important to take a step back and think, what are the ways in which employees that want to do harm can do harm using the technology?” she said.

For all the complexity the technology introduces, Diamond’s advice for HR leaders comes down to a few practical steps. “Number one is just know the technology is out there, be a little skeptical about what you’re being given, and don’t always accept everything that’s being given to you as accurate. Do a little bit more digging and probing to see whether you can find corroboration for it.”

RELATED INDUSTRIES + PRACTICES

- Artificial Intelligence
- Labor + Employment

©2026 Troutman Pepper Locke