Press Coverage | April 22, 2026

Leaked Client Data, Bigger Mistakes: Agentic AI's Hidden Risks for Legal Teams

RELATED PROFESSIONALS

William Gaus

Will Gaus, chief knowledge management and innovation officer of Troutman Pepper Locke, was quoted in the April 22, 2026 *Law.com* article, "Leaked Client Data, Bigger Mistakes: Agentic AI's Hidden Risks for Legal Teams."

> Will Gaus, chief knowledge management and innovation officer at Troutman Pepper Locke, told *Law.com* that the multistep nature of agentic processes can make it challenging to determine where things are going wrong absent well-placed checkpoints for human oversight.
>
> "If an early step is wrong, each subsequent step can build on that mistake," he noted. "The added complexity with agentic systems is that they can appear internally consistent even when they are wrong. Each step may logically follow the one before it, which makes the overall output harder to challenge if you are only reviewing the end result."
>
> …
>
> "Agents should operate within clearly defined boundaries, with limited and intentional access to data and tools," Gaus said. "Actions, especially those that move or expose information, should be constrained and in many cases require human review."
>
> …
>
> At a broader level, the potential efficiency gains of agentic systems can cause teams to deploy these tools before they've fully thought through the vulnerabilities they might expose and the steps needed to use them safely.
>
> "There is a tendency to push agentic systems into areas before the underlying processes, controls, and ownership structures are ready," Gaus said. "If a workflow is not well understood or consistently executed today, adding an agent on top of it can amplify the problem rather than solve it."

RELATED INDUSTRIES + PRACTICES

- Artificial Intelligence