PROTECTING TRADE SECRETS DURING TECHNOLOGY PILOTS AND VENDOR EVALUATIONS

August 3, 2026

A recent lawsuit filed by AI MCP gateway startup Runlayer against HR software giant Rippling is a reminder that a pilot program can quickly turn into a corporate espionage nightmare. According to the complaint, what began as a prospective customer relationship devolved into allegations of intellectual property theft. Runlayer claims it shared proprietary roadmaps, architecture, and source code over several months. When commercial terms fell through, Runlayer alleges it received a tip from inside Rippling that the company was building a near-identical competing product. Rippling has dismissed the claims as meritless. But whether or not the allegations hold up, the message is clear: if you hand over the keys to your kingdom for a test drive, you might be giving away more than you bargained for.

Runlayer and Rippling had the paperwork in place: a mutual NDA and a product trial agreement with explicit prohibitions against copying or creating derivative works. But too many companies believe that signed agreements are a suit of armor. They're not. Without careful planning and real-world safeguards, proprietary technology, processes, and business information remain exposed.

Define how confidential information may be used

An NDA without clearly defined permitted uses is like a lock without a key: it might look secure, but it's not doing the job. If you share access solely to evaluate a product, partnership, or acquisition, the agreement must say so explicitly and prohibit using that information to develop competing products or for any unrelated commercial purpose.

Don't stop there. Generic boilerplate doesn't cut it anymore. The agreement must address reverse engineering, competitive benchmarking, derivative development, and the use of information to train artificial intelligence systems. If you're relying on standard form language, you're playing with fire.

Limit access to what is necessary

Provide only the information and system access reasonably required for the evaluation. Sensitive source code, architecture, pricing models, customer information, and development roadmaps may not need to be disclosed during the earliest stages of a relationship.

Technical controls are essential, not optional. Access permissions, time-limited credentials, data-room restrictions, and detailed logs showing who viewed or downloaded information can supplement contractual protections, prevent misuse, and preserve evidence if a dispute arises. Courts look for real-world controls.

Document what was shared

Trade secret law rewards those who keep their secrets secret. A company asserting trade secret protection must demonstrate that the information was valuable because it was not publicly known and that reasonable measures were taken to maintain its secrecy. If you cannot prove you treated the information as confidential, the law won't protect it.

Businesses should therefore maintain records identifying:

- The information disclosed;
- The individuals receiving access;
- The purpose and duration of the evaluation;
- Applicable confidentiality restrictions; and
- When access was suspended or terminated.

Labeling confidential materials isn't just housekeeping, it's evidence. While labeling alone does not create trade secret protection, it helps establish that the company consistently treated the information as confidential.

Courts and juries notice.
Address what happens when discussions end
Don't assume the relationship ends when the pilot does. Agreements should include clear termination procedures: disabling system access, returning or destroying confidential materials, and confirming whether archival copies may be retained.

Here's the trap many companies fall into: they forget about backups, testing environments, and AI systems. Without addressing these specifically, your information may remain accessible long after commercial discussions have ended.

Coordinate legal and operational protections
Legal agreements and internal business practices must work together, not in silos. Business, legal, and information security teams should coordinate before beginning a technology pilot or sharing proprietary information with a potential vendor, customer, or strategic partner.

The time to figure out what was shared, who received it, and what restrictions applied is before a dispute, not after. Focus on the front end: prevention, documentation, and compliance measures working together to protect your trade secrets.

Berger Singerman's attorneys assist businesses with protecting intellectual property, structuring technology and evaluation agreements, and responding to suspected misuse of confidential information. Please contact a member of our team if you have questions about safeguards for an upcoming technology pilot, vendor evaluation or commercial transaction.

This article is provided for informational purposes only and does not constitute legal advice. The information should not be relied upon as a substitute for advice from qualified legal counsel. No attorney-client relationship is created by this article. Readers should engage and consult counsel regarding their specific circumstances.

Related Team Member(s)

Geoffrey Lottenberg