

4 Tips To Avoid Landing In Trade Secrets Hot Water

By **Bill Donahue**

Law360, New York (July 09, 2014, 7:09 PM ET) -- Companies are getting smarter about protecting their trade secrets alongside the rest of their intellectual property, but they also need to be equally wary about accidentally stealing somebody else's.

With high-profile criminal cases, dramatic overseas accusations and the talk of new federal legislation, companies are more aware than ever of the importance of locking down the kind of highly valuable secrets — customer lists, unpatented processes, source code — that drive their business. But that's only half of the equation. Without proper precautions, a marquee lateral hire or a failed attempt at a joint venture can leave companies with a wholly different risk: a product tainted by a competitor's trade secrets, negative press and costly litigation.

Though perhaps not as bad as losing your own secrets, no company wants to end up on the wrong end of a misappropriation suit.

“Over the last three to five years, trade secret protections have become a more important body of law, and companies are getting more focused on protection of their own information, but now we're counseling that clients also get equally focused on making sure that their own products are not tainted,” said Mark A. Klapow, a partner at Crowell & Moring LLP.

“These big trade secrets cases that involve competitors and key products are very expensive to litigate,” Klapow said. “Just as in a large patent case, there can be tens or even hundreds of millions of dollars at stake.”

Good written policies and other standard measures are a must, but here are a few quick tips from the trade secrets attorneys in the trenches:

Be Extra Clear in Hiring

Any on-boarding policy worth its salt should include explicit warnings about noncompetes and bringing over any material at all from a prior employer, including requiring written representations that the rules are being followed. But there are times when even that's not enough.

Some employees might think the legalese warning they signed was just a formality, something in the standard procedure, but that their new company really still wants them to lean on something beyond just their talents, such as old customer contacts or knowledge of proprietary formulas.

“You need to make sure that message is coming not just from a high and mighty level but from day-to-day supervisors: ‘We don’t want anything from a prior employer,’” said Victoria A. Cundiff, the chairwoman of Paul Hastings LLP’s global trade secrets practice. “One way is have an entrance interview, to say, ‘We weren’t just winking and nodding. We don’t want that stuff on your thumb drive.’”

Other pitfalls are more subtle, like a new hire who isn’t quite clear that the work product they created for the old company isn’t theirs to keep.

“It’s not done maliciously, but sometimes, new employees, especially in the tech space, have a sense that since they worked on it, they have a right to take it with them, even though they signed documents saying otherwise,” said Robert Shwartz, a partner with Orrick Herrington & Sutcliffe LLP.

“In a serious way, people should be told that they should not be bringing anything at all unless they were given express permission to do so,” Shwartz said.

Avoid Business Temptation

Another big limitation for well-crafted policies aimed at preventing misappropriation is pretty simple: companies bending the rules — or ignoring them entirely — when the business reward is big enough. In some cases, that means bringing on a marquee hire from a competitor despite red flags; in others, it means integrating a new employee onto a key project faster than they should.

“It’s nice to have it on paper, but you need to make sure you actually follow your policies, that you don’t allow the business leaders to compromise what the legal teams have already decided is the best way to protect the company,” said Robert B. Milligan, a partner with Seyfarth Shaw LLP.

“There’s a measured solution to each employee hire, but it can’t just be that you want to get away with something,” Milligan added. “You can’t put your head in the sand and just hope something bad doesn’t happen.”

The same thing can very easily happen in failed mergers and acquisitions or in joint ventures that have run their course. It’s understandable: A company was thinking more about sealing a lucrative deal than accidentally tainting itself with someone else’s trade secrets.

“In these situations, there is often a tension between business goals and legal obligations, between the drive to close a deal and the duty to protect confidential information,” said Randall E. Kahnke, a partner with Faegre Baker Daniels LLP. “If you are going to compete in the same space with your former business partner, have you thought about who within your organization may and may not have access to the confidential information you receive?”

When In Doubt, Quarantine

One key to the entire preventive effort should be creative solutions for quarantining or cordoning off potential sources of outside trade secrets from the rest of the company to prevent them from tainting the wider organization.

It might be obvious to do that with a riskier new hire — have them sit out on big projects for six months after coming over from a direct competitor — but it’s less so in other areas, like the interview process

itself.

“It's important who is part of the interview process and whether they've been coached,” Milligan said. “If your interviewers are engineers or sales managers, and they start talking about technology or customers, that's rife with exposure.”

On the deals side, one thing to consider is using so-called “clean room” techniques: isolating certain engineers or developers from the partner company and its information for certain projects, providing useful defensive ammo if the former ally becomes a litigious competitor.

“Your former business partner is now your competitor. You have been exposed to their confidential information,” Kahnke said. “If they accuse you of improperly using that information, will you be able to demonstrate that you developed your competing product without using that information? Following clean-room procedures is one way to create powerful evidence of independent development.”

Educate — Through Horror Stories

Making everyone aware of the shared consequences of misappropriating another company's proprietary information — stalled projects, burdensome investigations, termination of employees and personal and corporate liability — is an effective way to spread the policing around an organization.

It's easy to ignore jargony terms in a legal document; it's tougher to ignore training and education programs that give employees on all rungs of the ladder a real-world glimpse at what happens if they don't follow the rules, experts say.

“Nobody wants to be the next example of what goes wrong,” said Paul Hastings' Cundiff. “We often tell clients: Here are some horror stories you can pass on.”

Cundiff relayed one such story that involved a generic pharmaceutical company that was on the verge of releasing a drug after the patents had expired, only to be forced to hold off after it got mired in trade secret claims by bringing over former employees from the pioneer drugmaker.

“It had a huge impact on the financial picture of the company because the excellent safeguards hadn't been followed,” Cundiff said. “That kind of story is really powerful to share with clients because the consequences can really be devastating.”

--Editing by Elizabeth Bowen and Christine Chun.