

Chicago Daily Law Bulletin®

Volume 157, No. 27

Tuesday, February 8, 2011

IP lawyers help clients protect trade secrets

By Amanda Robert
Law Bulletin staff writer

While the explosion of trade secrets dates back to the early 1980s and the birth of computers, more companies depend on this intellectual property right as protection for their assets in an increasingly information-based society, said R. Mark Halligan, an IP partner at Nixon, Peabody LLP.

"Companies are recognizing that in order to maintain a competitive advantage in the marketplace, they have to get serious about trade secrets," Halligan said. "It's an asset that is often swept under the rug in what I would call the industrial revolution era, where the primary IP asset was patents."

"But now, we have all sorts of information assets, all the way from research and development information to customer information and everything in between," he said.

Despite the growing use of trade secrets, companies need to be more proactive about properly protecting and enforcing them, Halligan said. They introduce policies that prohibit employees from exposing trade secrets, but they don't always train their employees on what information should or should not be discussed with suppliers or customers.

"If you take information that has the status of a trade secret internally and disclose it to a third party without an obligation of confidentiality, the status on the information is lost instantly," Halligan said. "Like taking a pin and pricking a balloon, it's gone."

Companies used to catch employees who purposely stole trade secrets after watching them carry out briefcases of paper or copy large amounts of documents, Halligan said. Now, employees can take the entire company on their thumb drive or transfer confidential information through their private e-mail accounts.

David M. Airan, an IP attorney at Leydig, Voit & Mayer Ltd., said any time a key employee leaves a company and heads to a competitor, the company should search its computer system to determine if the employee took any trade secrets.

"A lot of times you're able to determine through a computer forensic analysis whether there was suspicious activity," Airan said. "For example, you might see massive copying of a database, you might see massive deletions that are suspicious or you might see a certain file deleted and deleted again — not just deleted from a program, but also the recycling bin will be emptied."

Eley O. Thompson, another IP attorney at Leydig, Voit & Mayer Ltd., works with Airan to counsel clients on how to best protect their trade secrets. They advise companies to involve both general counsel and information technology groups in identifying trade secrets and implementing data-loss prevention software to control employee use of information.

"All of us agree that the biggest potential problem comes from insiders," Thompson said. "All of the companies are pretty good at setting up firewalls to keep the outside from getting in; it's the insider who is the problem."

Halligan, who also helps his clients set up trade-secrets protection programs, recommends that companies restrict confidential information to key employees and use electronic security codes to further protect information.

He also suggests that clients add a trade-secret portion to employee exit interviews. The company should put together a list of projects that involved sensitive information and require employees who leave to sign documents stating that they will not disclose information from those projects.

"Later on, when it turns out that he has the whole company on his home computer or that he is involved with a direct competitor, you have this agreement to demonstrate to the court that there was a breach of company obligations," Halligan said. "That's a simple how-to technique you can implement overnight, which makes a huge difference in litigation."

Gregory J. Vogler, a shareholder and co-founder of McAndrews, Held & Malloy Ltd.,

who primarily handles patent, trade secret and trademark litigation, said he saw more companies get involved in litigation over trade secrets in the past five years.

"If someone rips you off, leaves your company with information, and you suspect that, you sue them for civil action and also seek criminal action against them if it falls within criminal statutes," Vogler said. "The combination of using computer-monitoring capabilities, common sense in protecting and limiting access and being forceful in enforcement of the rights tends to keep most employees in line."

When Vogler represents large corporations in business deals with smaller companies, he also works to prevent future litigation that arises after companies fight over the origination of ideas.

"Before a large company signs an agreement to get access to another party's confidential information, I make sure a provision says that if companies do not make a deal and go their separate ways, the only relief that the small company would get against the big company is through patents, trademarks or copyrights," Vogler said. "You don't have to fight the battle of who came up with the idea when and what did you learn. It's just a big mess. The small individual always thinks the large company takes their idea, when in fact, most of the time they do not."

When Vogler represents the smaller company, he accepts that provision, but he also requires the large company to destroy or return all information related to his client, including any notes, he said.

"If companies did those things, it would resolve a lot of lawsuits," Vogler said. "The purpose is to avoid stupid disputes based on someone being upset that the deal didn't go through."

"If you do have a dispute, it should be a concrete dispute based on a patent, trademark or copyright or on a specific requirement in the agreement that's easy to understand and enforce."