Focus

LOS ANGELES DAILY JOURNAL • FRIDAY, NOVEMBER 21, 2008 •

Secrets Service

By Benjamin K. Riley

It's Friday afternoon. One of your most important clients calls and says that its key technologist is leaving the company and is starting a similar job with a competitor on Monday. The client believes that many of the company's most important trade secrets will go with him. What do you do?

Make sure that the company human resources personnel conduct and properly handle the exit interview. Have the employee reaffirm his obligations under his employment and confidentiality agreement. Itemize and document all company property returned by the employee, including his computer, PDA and all electronic and hard document files. Ask about the employee's home computers and request to have a third party inspect them. Consider having at least the general counsel at the exit interview, and possibly outside trade secret counsel. Make it very clear that litigation will immediately result if any trade secrets or other company property are taken to or used at the new employment.

Think about how to prove that the secret or process 'provides economic value,' whether the information is known to others or easily discovered, and whether the company has adequately protected the secrecy of the information.

Immediately secure the employee's computer. Hire a forensics expert to image the computer's hard drive that weekend. (Outside counsel or one of the major document processing companies can recommend one.) Do not attempt to start up the computer to investigate the files yourself; the computer should be preserved in its current state for evidence.

The company's investigation of any copying, sending or taking of trade secrets should be conducted from the image of the computer's hard drive created by the forensics expert.

Start investigating the company's documents and records to determine if anything has been taken. Review company logs that may indicate any usual copying by the employee, shipping of documents and late-night or weekend visits to the office. If you find such evidence, consider checking company video cameras for visual proof. Interview co-workers.

Talking to co-workers serves the dual purpose of gathering evidence of possible trade secret theft, and letting co-workers know that the company is serious about preserving and protecting trade secrets. And thoroughly check the forensic image of the former employee's hard drive and e-mail.

Send a demand letter (perhaps sent by outside trade secret counsel) to the former employee and new employer, advising them of the employee's continuing confidentiality obligations under his employment and confidentiality agreement and the company's intention to vigorously protect and enforce its trade secrets. A demand letter almost always makes sense if a company has suspicions of trade secret or property theft. It puts the new employer and former employee on full notice of the seriousness of the situation, and helps create the record if actual or threatened misappropriation is later found.

Trade secret litigation is technical, expensive and full of traps for the ill-prepared. Consider if there are other legal theories such as breach of the employment and confidentiality agreement, or breach of fiduciary duty, that might meet the company's goals. Are there alternative forums for the case? Although approximately 45 states have adopted the Uniform Trade Secret Act, there are differences in the respective states' enactments. For example, California requires service of a detailed trade secret statement (Code of Civil Procedure Section 2019.210) at the outset of discovery, presenting an immediate, major challenge. Perhaps another venue or legal theory would be preferable in the case.

Carefully review the requirements for proving a trade secret to see if the company has any immediate issues in establishing a case. A trade secret is: information, process or technology that provides economic value to the trade secret holder; not generally known to others and not readily ascertainable by proper means; and subject to reasonable measures to safeguard secrecy.

Think about how to prove that the secret or process "provides economic value," whether the information is known to others or easily discovered, and whether the company has adequately protected the secrecy of the information. Apart from whether anything has been misappropriated, defendants often challenge the company's security measures. Consider: Does the company have signed and periodically reaffirmed confidentiality agreements with both employees and vendors; are trade secret files and documents protected by passwords, marked confidential, limited to people with a need to know and/or otherwise adequately safeguarded; what information has been published or made publicly available about the trade secret information; have facility or office tours or other visits been allowed, and if so, to whom (customers, competitors, vendors, etc.); are technical drawings adequately secured?

In California and most federal courts applying California law, before technical discovery can proceed, the plaintiff in a trade secret case must first serve a statement describing its trade secrets with reasonable particularity.

Although not adopted elsewhere by statute, many other jurisdictions will require a similar statement; if not, you can be sure the defendants will ask for a detailed description of the allegedly stolen trade secrets by way of interrogatory. A trade secret description also will normally be required to obtain a temporary restraining order. Plaintiffs can make a serious mistake by doing a poor job on the trade secret statement. A detailed and full description of the trade secrets, often supported by detailed attachments, is essential. Conduct intensive interviews with the company's technical employees and have them assist in the identification and description of the trade secrets.

A careful trade secret plaintiff will prepare the trade secret statement at the very beginning of the case, as part of drafting the complaint. Remember, if an inadequate trade secret statement is prepared and served, the other side will likely attack it

and the judge might delay or deny technical discovery, and even reconsider granting a temporary restraining order.

Consider and discuss any protective order issues. The Section 2019 trade secret statement and the supporting technical documents will have to be produced to the other side — the very persons you claim want to steal the trade secrets. Attorneys'-eyes-only provisions in the protective order provide protection, but often at least one in-house counsel will need to be privy to confidential or even highly confidential documents.

Discuss these issues with your client. They need to understand that you may not be able to share with them all the details you discover about the opposing company's technology and conduct since it might be protected as highly confidential. And consider that even the protective order safeguards may be lessened or dropped if the case goes to trial since the judge may require a public trial and an open courtroom. Note also that although the client's engineers will be the key resource for drafting your trade secret statement, you will not be able to discuss and obtain their guidance on technical information you learn during discovery from the other side. You will only be able to share the opponent's technical information with your legal team and experts.

The strength of the case will depend in large part on the strength of your trade secrets. Precisely defined technical trade secrets will generally be afforded the most protection by courts. Support them with schematics or engineering architecture documents. Business trade secrets will be enforceable as well but keep them precise and pertinent to the most confidential business data or corporate opportunity documents.

The strongest (and perhaps rarest) case features proof of actual misappropriation of trade secrets and integration of the trade secrets into the opponent's product. Proof of actual misappropriation alone will likely entitle the company to an immediate temporary restraining order to stop any actual or further use of the information. When actual misappropriation has not yet been established, injunctive relief is still available for threatened misappropriation, especially when coupled with acts of duplicity or culpability by the former employee. The inevitable disclosure doctrine has been rejected in California, but is good law in the majority of jurisdictions (for example, Arkansas, Delaware, Illinois, Minnesota, New Jersey, Ohio, Utah and Washington). Some states such as Connecticut, Iowa, Massachusetts, New York, North Carolina and Texas have adopted the inevitable disclosure doctrine only for technical trade secret cases. Again, think about the advantages of the various jurisdictions where the case may be brought.

At the outset of the case, consider the ultimate goal. In a jurisdiction such as California, which has rejected the inevitable disclosure doctrine or in which covenants not to compete are generally unenforceable, chances are the company will not be able to prevent the employee from working in his or her area of expertise. Nonetheless, in most cases a temporary restraining order will limit the damage to the company and prevent a competitor from obtaining an unfair advantage through trade secret theft.

And if the trade secrets are ultimately incorporated into a product the new employer brings to market, the original employer has a strong unjust enrichment case. Finally, trade secret actions and associated injunctions demonstrate to a company's existing employees and the market that the company is serious about protecting its trade secrets.

In most trade secret cases, actual damages are difficult to establish. Especially with a technology start-up, it's hard to prove that the original employer lost actual sales due to trade secret theft by a former employee. Instead, most cases will focus on the unjust enrichment to the new employer of incorporating stolen trade secrets, thereby bypassing a long development process. Damage studies will focus on the time and expense saved by the defendant to get to market as a result of the trade secret theft. In a case with multiple trade secrets, consider the head start provided to the defendant from stealing the trade secrets both on a collective and an individual basis. That way, the jury will have a basis on which to assess damages if it finds theft of fewer than all the trade secrets.

Trade secret cases offer fast-moving, important and interesting litigation. Be ready for that Friday afternoon call.