Legal Times
WEEK OF OCTOBER 23, 2006 • VOL. XXIX, NO. 43
ALM

So You Think They Got Your Secrets?

When groups of employees move over to a competitor, in-house counsel need to act fast.

By W. Michael Holm

You are the in-house general counsel of a sizable high-tech company. One Monday morning, your CEO and CFO walk into your office together. That's never a sign of good news, and in this case, the news is troubling indeed.

Both executives strongly suspect that a former senior-level employee, who recently left the company, is working with a competitor to raid your company's employees and to exploit your company's confidential information or trade secrets. They report that several other employees resigned last Friday and are expected to join the senior employee any day. The CEO and the CFO want you to do something about this—and quickly.

Corporate Counsel
A Special Report

Sound familiar? This pattern repeats itself frequently in today's competitive business environment. And when it does, the former employer often experiences significant financial losses, not only from the loss of valuable confidential information but also because of the loss in productivity and the expense of retraining caused by the loss of key employees. The first question the CEO asks you is, "Is this legal?" In many cases, the answer is "No." And the second question is, "What can we do about it that will protect our company and send a message to existing employees that we will not tolerate this kind of conduct?" The answer to that question is often more complicated.

Can They Do That?

There are many bases upon which conduct of this sort can be deemed illegal. Many companies include in their employee contracts noncompete and nonsolicitation clauses that, if narrowly drawn, are enforceable. In addition, such contracts frequently contain confidentiality provisions that restrict employees from using confidential information after their employment ends. Even in the absence of such clauses, however, most states and the District of Columbia recognize a number of common law and statutory duties that can help a company gain redress against a rogue employee.

First, all employees, including officers and directors, owe their employers a fiduciary duty of loyalty. This common law duty requires that the employee exercise the utmost in good faith and loyalty toward the employer and precludes the employee from acting in a manner adverse to the employer's interests. This prohibits the use of the employer's confidential or proprietary information after termination to aid a competitor; usurping corporate opportunities, that is, personally taking advantage of a business opportunity that belongs to the company; and soliciting an employer's clients or employees prior to resignation. While employees are generally allowed to make arrangements to resign and compete with their current employer, if the resignations are part of a coordinated plan that is likely to result in significant harm to their current employer, their conduct may violate their fiduciary duties.

Similarly, if the new employer is complicit in making the arrangements for the group of employees to switch employers, it may be charged with aiding and abetting a breach of fiduciary duty, thus making it jointly liable for damages.

In addition, the departing employees and the new employer may be charged with interfering with your company's contracts with its employees and clients, if those relationships have been affected. Even if your employees are at will, neither competitors nor former employees have any right to interfere with those contracts.

In this area, if the employees have misappropriated your trade secrets, Maryland, Virginia, and the District of Columbia all provide remedies that include damages and injunctive relief under the Uniform Trade Secrets Act.

Finally, if you are in Virginia, the Virginia Business Conspiracy Statute is a big gun in the arsenal of any corporate counsel. Under the statute, it is illegal for employees or competitors to conspire to injure your business. To prevail under this theory, you would have to prove that your former employees, by themselves or with the competitor, acted intentionally,

purposefully, and without legal justification to injure your company. A breach of fiduciary duty or assisting in such a breach satisfies the requirement that the conduct be without legal justification. Moreover, injury to the plaintiff need not be the overriding purpose of the defendants' actions; all that is required is that they knew injury would result. Success under this theory entitles you to recover treble damages and attorney fees.

So, armed with all of these legal theories, can an in-house attorney help his company win this case? The proof is often hard to uncover. But there are some practical steps you can take internally to investigate what has occurred. First, once you reasonably anticipate that litigation may occur, the law requires that you place a "litigation hold" on all relevant documents and electronically stored information. That is, you must not allow the destruction of information that would potentially be discoverable should the company sue the departed employees. This may require suspension of your company's document retention policy, at least in part, during the duration of the case.

Second, you should preserve all backup tapes from the period you suspect planning for the new venture began to the present. Those tapes should be reviewed by a forensic examiner, and all e-mails and user files for the employees at issue should be extracted and examined. If you suspect that other current employees may leave or may have been solicited to do so, examine their e-mails as well. In general, the law does not recognize any expectation of privacy in e-mails sent or received from a company's computers.

Third, if the departed employees used desktop or laptop computers that contained hard drives, make forensically sound images of the hard drives. Ask the forensic examiner to provide an index of the contents of those computers, including those user files and e-mails that have been deleted. If possible, restore the deleted files. Even if they can't be restored, examining metadata can often reveal when the deleted files were created, last accessed, and last modified.

Fourth, if your company records numbers for all telephone calls received and initiated from particular extensions, isolate the information for the employees at issue over the relevant time period and look for patterns of calls among them. Pay particular attention to calls made to or from the office phones and key employees' cell and home phones. Do not tape any phone calls. Rather, examine the telephone numbers associated with calls made and received.

From this information, you may discover e-mails and planning documents related to the employees' departure and future employment. You may also find that certain proprietary information or trade secrets that would not normally have been saved to their hard drives had been deleted or e-mailed to their home computers or those of their co-conspirators. And, you may discover evidence of meetings attended by groups of employees where planning for the new venture may have occurred.

Experience has shown that employees who leave as a group or within a short period of time to found or join a rival firm are careless. This may result either from greed or an unwillingness to incur any significant financial risk; or from pressure applied by the new employer to bring with them sufficient work and clients to be profitable within a short period of time. Consequently, they frequently abscond with proprietary data.

Before filing suit, however, send a cease-and-desist letter to all of the former employees as well as their new employer. Include in that letter a demand that they protect from destruction any documents and electronic files in their possession that may be requested in discovery. Once you have done that at an early stage, electronic information becomes subject to the "litigation hold" requirement.

Digging Deep

At the time you file suit, serve initial discovery requests on the defendants with the complaint. Among the things requested, ask that they produce all home and cellular telephone bills for the period in question, and seek a forensically sound bit map image of the hard drive in all computers in their possession from which relevant e-mails and user files may be extracted.

Propose a protocol and search criteria for the production of electronic information that requires that it be produced in a searchable format with metadata included. Don't accept a hard-copy production of electronic data. If the defendants will not promptly agree to a protocol, ask the court to adopt the one you have proposed.

Don't be surprised if the individual defendants balk at the cost of copying and examining their hard drives. Given the volume of data the drives likely contain, this cost can become significant. Because very few documents exist any longer in paper form, this type of discovery may become pivotal in proving your case. Be prepared to pay the costs associated with the data extraction, so long as you are entitled to shift costs back to the defendants if relevant electronic documents are discovered.

Once your forensic examiner has the defendants' hard drives, ask the examiner to determine what may have been deleted since the preservation letter was sent to the defendants or the earliest date when they knew litigation was reasonably anticipated. Also, seek an index of the user files found on the hard drives. This will enable you to have the examiner pull specific documents that are responsive to your discovery requests.

If the examiner locates specific files or e-mails that were deleted during the "litigation hold" period, the affected defendants may be subject to a spoliation charge. If spoliation of potentially relevant information is proven, the available penalties include monetary sanctions, an adverse-inference instruction, dismissal of any claim brought by the defendants, and a default judgment.

At the same time you are seeking discovery from the defendants, subpoena their phone records (cell and home) from the appropriate carrier. Cell phone records, in particular, may enable you to track and prove the conspiracy. Some bills even provide the geographical location of the calling party, potentially useful information if travel was involved.

If the individual defendants have joined an existing company, seek all e-mails during the critical period between those defendants and people at the new employer with whom they had contact during the period in question. Similarly, if a new venture is involved, subpoena the e-mails between the defendants and vendors that were necessary to a successful launch of the new venture.

The odds are that, even if the individual defendants have deleted their e-mails, they will remain on the recipients' servers. If anything is certain in this electronic age, it is that "e-mail lives forever." The plaintiff's counsel must be diligent in searching for possible third-party sources of e-mail communications. The results are usually worth the effort.

The costs of this type of litigation will be high, and you may need to reassure your CEO and CFO that it's worth the time and money. If there have been serious employee defections, however, and your company has suffered significant monetary losses, litigation may serve several ends.

First, it may stop defections, facilitate an agreement by the defendants not to continue to use trade secrets, and allow you to recover your financial losses. Second, it will serve as a strong signal to the remaining employees that your company will aggressively protect its intellectual property and valued employees. In sum, an aggressive investigation coupled with creative lawyering by in-house and outside counsel will likely result in a positive outcome for your company.

W. Michael Holm is a member of Womble Carlyle Sandridge & Rice, working in its Tysons Corner, Va., office. He is a member of the firm's business litigation practice group and can be contacted at mholm@wcsr.com.