TEXAS LAWYER

Lucky 13: A Baker's Dozen of Tips for Stopping a Departing Employee from Using Protected Company Info

April 14, 2014

Companies rely on their lawyers to protect their trade secrets. As such, lawyers must be prepared to investigate whether a departing employee has wrongfully taken or misused company information and, if so, determine why.

Some employees mindlessly copy their project files before returning their company laptop, but others take information with a specific plan to help themselves or their future employer. Both require a quick response.

This checklist will help lawyers discover, address and resolve both scenarios. Lawyers promptly should take these steps because a court is less likely to grant relief if it perceives that a company is slow in responding to security breaches.

1. Interview the departing employee. When dealing with an employee suspected of wrongfully taking company information, two potential trial witnesses should conduct the exit interview. At least one should be personally familiar with the departing employee and his job responsibilities, and one should take detailed notes. Otherwise, the departing employee may dispute the content of the discussions.

During this interview, uncover: 1. the employee's efforts in finding a new job, particularly with competitors, to reveal specific disclosure risks, 2. whether and how his future plans may include competing with the company in areas involving information to which he had access, and 3. whether the employee admits to retaining files that he should have returned.

To overcome any hesitancy by the employee to talk openly, explain that identifying potential problems is an important step to resolving the issues.

2. Forensically examine company-issued laptop and server activity. Evidence that the departing employee electronically downloaded confidential company information to an unauthorized device is usually critical circumstantial proof of potential misappropriation.

Such evidence should prompt a focus on discovering and retrieving copies of the information and remedying any misuse. An in-house forensic examiner could testify definitively to what the departing employee did.

3. Hire a law firm. If at this point there are concerns that company information has been stolen, retain a law firm.

4. Issue a litigation hold memo. Departing employees who a company sues often look for any counterclaim to leverage in settlement. Therefore, besides customary litigation hold instructions, the

memo should caution recipients against discussing the case except through legal counsel, since communications that take place outside of litigation preparation are potentially discoverable and may serve as the basis for a defamation or interference claim.

5. Interview knowledgeable employees. Interview all knowledgeable employees who receive the litigation hold to confirm compliance, gather the facts and identify the best witnesses to explain the seriousness of the potential security breach.

6. Send a letter to the departing employee's future employer. In the letter, request assurances that the future employer will take reasonable steps to prevent receipt or misuse of the company's confidential information. The letter should not make definitive factual statements that may turn out to be defamatory.

For example, don't state that a departing employee "stole" confidential information with the intent to misuse it. Rather, allege that he "apparently copied" confidential information that may be misused with significant consequences. The objective is to avoid a potential problem, not cause one.

7. Prepare a lawsuit. Draft the lawsuit, but do not file it until after determining that litigation is the more expeditious way to deal with the departing employee. Usually, a lawsuit diminishes the opportunity to maintain the departing employee's cooperation, and he may retain a trial lawyer, through whom the company must direct all further inquiries.

8. Seek a TRO application and affidavit. If litigation is required and the company has acted promptly and can show through a detailed affidavit that the employee took confidential information and now is in a position to misuse it, a court often is willing to enjoin the departing employee for a few weeks to preserve and not misuse confidential information.

9. Engage a third-party forensic examination witness. A third-party testifying examiner can help prove that the departing employee stole information. Computer forensic witnesses vary greatly in cost and experience. Which to choose will depend on the amount in controversy and the anticipated issues.

10. Move for expedited discovery and forensic examinations on the employee's devices. To prepare quickly for a temporary injunction hearing, seek narrow, expedited discovery. That should included the opportunity to depose the most significant witnesses, a chance to obtain documents relating to the employee's efforts to leave the company and a forensic examination of all devices that held the confidential information. Also, seek entry of a protective order.

11. Temporary injunction hearing. At the hearing counsel will need to present at least one or two witnesses, and perhaps a forensics expert, who can testify directly that the departing employee wrongfully took company information that is: unknown outside the company, and perhaps even to most employees within the company; reasonably protected by the company; and valuable in the business, requiring significant money or effort to discover or develop. The company also must explain why unauthorized use or dissemination undermines the value of the trade secret or otherwise harm the company.

12. Respond to appropriate settlement overtures. By the time a temporary injunction is entered or denied, the parties have expended significant effort and should have a good idea of the facts and the court's perspective. If they haven't started already, it's time to talk settlement.

Common settlement terms include an agreed injunction with a scope similar to the requested temporary injunction, contractual obligations to obey the injunction and not misuse or disseminate

confidential information, representations concerning the defendant's past and present use of the confidential information, and forensic examination of any other defendant storage devices to confirm no confidential information.

The defendant will want to limit future discussion of the lawsuit, to protect his reputation. Resist these efforts to deter future thefts.

13. If needed, proceed through final trial and appeal. If the company and the departing employee can't settle their dispute, then the case must proceed to trial.

By the end of the process, current employees should perceive rewards for cooperation and consequences for deception and recklessness.

Anna Rotman is a trial partner in Yetter Coleman and president of the Harvard Law School Alumni Association of Houston. She handles contract, business-tort and antitrust claims for plaintiffs and defendants.