5 Things Employers Must Do When A Key Employee Leaves

Publication
5.02.17

With ever-changing technology, employers must be more conscious than ever of protecting trade secrets and customer relationships when an employee decides to leave, especially if the departing employee is joining a competitive business or starting their own competing venture. When a top salesman or other key employee leaves, employers sometimes become frazzled and neglect to take steps to preserve and protect confidential information. By instituting the five simple steps outlined below, employers and their counsel can ensure they preserve and protect confidential information when the top dog decides to leave the company.

Step 1: Exit Interview

The exit interview is often overlooked and underutilized, but it provides employers with a chance to gather as much information as possible relating to the departing employee's future plans. In the exit interview, not only can an employer determine the employee's future employment plans, but it can remind the employee of his employment agreements, and determine whether he possesses confidential information. Many managers dread these interviews because they want to avoid what they assume will be a confrontation. But when done in a cordial manner, employers can often gather information most effectively through an interview.

An exit interview should be a nonhostile conversation covering the employee's time at the company. It is the perfect time to not only learn the pros and cons of your company and management, but to determine what, if any, proprietary or confidential information the departing employee has in his possession.

Employers may inquire about the departing employee's conduct leading up to the resignation, including whether the employee has shared confidential or proprietary information (particularly with a third party, i.e., his new employer), or whether he has advised any customers (or coworkers) of his plans to resign. This can also be an opportunity to remind the employee of the requirement that he must return all property and proprietary information belonging to the company that he has in his possession. While it is appropriate to remind the employee of his legal obligations and requirements, we recommend reviewing these items with him at a later step (see step 5), separately from the exit interview.

Depending on what is learned in the exit interview, the employer may decide not to allow the

Depending on what is learned in the exit interview, the employer may decide not to allow the employee to remain employed during any "notice" period. For example, if a top salesman provides two weeks' notice, but his activities are suspicious and he plans to work in the same capacity for a competitor, the prudent course may be to end all formal activity and immediately cut off his access to company information (see step 3 below). Most employers in this situation will pay the employee's remaining salary during the rest of the notice period, though in Texas, like most states, this is not required unless there is the equivalent of a contractual arrangement established through the company's policies.

Step 2: Document Assembly and Review

Employers should gather all of the departing employee's signed employment agreements and review them to determine whether the employee's future plans, as discussed in the exit interview, violate any of his signed agreements, particularly noncompete and nonsolicit covenants. This step may be done before the exit interview.

Step 3: Call Information Technology

After the employee leaves, employers should have the IT department do an examination of the person's email in order to determine whether he has been forwarding anything to his personal email account. This is an easy process for IT to complete. Employers should do this for every departing employee that was in possession of critical company information and in a position to harm the company by misusing it.

Additionally, if not already completed, have IT immediately terminate the employee's access to company systems, including remote access and voicemails. Most businesses know to terminate the employee's access to their network and email accounts but often overlook other ways former employees have access to the employer's network.

Step 4: Preliminary Examination of Hard Drive

If the employer has a heightened concern about a particular employee, the employer should conduct a deeper inspection of the hard drive in the computer used by the departing employee. Companies do not typically have the time or resources to conduct deep-dive investigations into the computer of every employee that leaves, but should do so for those whose departures do not pass the "smell test." If an employer believes there is a risk that the departing employee has taken something proprietary, a thorough examination of the computer is warranted. Employers can start by directing the IT department to image and/or clone the employee's hard drive, which creates an exact replica of the computer. Additionally, a simple internet history search may lead to damaging information (e.g., departing employee searches "how to get away with stealing company information").

Another option is to conduct a registry examination and report. This report, which can be accessed by a number of tools, provides a history of every device (e.g., USB, flash drive, smartphone, external

by a number of tools, provides a history of every device (e.g., USB, flash drive, smartphone, external hard drive) that has been put into a computer, including the time the device was inserted into the computer, the device's manufacturer, and even the device's serial number. It would certainly be an eyebrow-raiser if a departed salesman inserted a USB into his computer the day before he left. If additional tests reveal that a salesman was accessing important customer information at the same time an electronic storage device was inserted into a USB port (particularly material that he did not regularly use or had no reason to access right before his departure), red flags will be flying high.

Computer forensic experts have the ability to review software installed on the computer, which can reveal use of cloud storage sites, such as iCloud or Dropbox. Experts would also be able to see if the employee used software designed to hide evidence of misappropriation. Moreover, experts can trace "deleted" files. "Deleted" files are not always deleted; files could be held in the trash bin, or even if deleted, the data is not always permanently erased unless expressly overwritten.

Typically, cost-conscious companies choose to recycle former employee's computers. While this saves time and money, employers should refrain from immediate frugality in cases of heightened suspicion and preserve the computer in order to conduct testing. If the employer instantly recycles the computer for the next employee, it may be deleting evidence of misappropriated confidential information. Abide by the following motto: examine first, then recycle.

In March, the Texas Fourth Court of Appeals in Christopher Michael Hughes v. AGE Industries Ltd., showed just how beneficial steps 4 and 5 can be for employers. In this trade secrets misappropriation case, AGE Industries (AI) learned that the month before Hughes left to join a competitor, he downloaded a large amount of data from his work computer and had confidential AI information on his personal computer. During the temporary injunction hearing, AI presented a third-party contractor's report, which showed that Hughes downloaded a large quantity of data from his AI computer onto a USB. Moreover, Hughes could not testify that emails he sent to a now co-worker did not contain AI's confidential information. The court upheld the lower court's temporary injunction, preventing Hughes from using or disclosing AI's proprietary or trade secret information, finding that AI was not required to show actual use of trade secrets; rather it had to show Hughes had possession of the trade secrets and was merely in a position to use them. Because AI had evidence that Hughes had possession of the data by downloading it onto a USB, Hughes was therefore in a position to use this data, and AI's temporary injunction was granted.

Step 5: Communicate Regarding Obligations

Step 5 may seem like a repeat of step 1, but communicating with the departing salesman regarding his obligations is more effective if completed separately from the exit interview. Exit interviews are congenial and for the purpose of gathering information, whereas reminding former employees of their restrictive covenants can sometimes lead to confrontation.

To emphasize the importance of the employee's obligations, have him sign a document confirming a number of exit issues, such as: (1) the employee had access to employer's confidential information

number of exit issues, such as: (1) the employee had access to employer's confidential information during his employment and will not disclose that confidential information; (2) the employee's acknowledgement of his signed employment agreement; (3) the employee's acknowledgment of any and all covenants and obligations he has to the employer; (4) the employee has returned all company property (including hard copies of any and all customer and company proprietary information); and (5) the salesman is aware that the employer expects full compliance and will enforce all contractual and common law rights against him, if necessary.

To avoid ambiguity, create a checklist that the departing salesman can initial to acknowledge each point. This step not only affords extra coverage for employers, but likely creates a deterrent if the salesman is considering breaching his employment contract.

There are two ways to communicate to the departing employee about his obligations. Employers can have a nonadversarial conversation with the departing salesman explaining his obligations and informing him that the company has or will review everything relating to him: his computer hard drive, emails and executed employment agreements. The other way to communicate these obligations to the salesman, albeit less cordial, is via a demand letter. This step is recommended only when there is at least some evidence that the employee has already crossed the line or expressed an intention to disregard his obligations. By following the steps outlined above, employers can take greater control in protecting information that would be fatal in the hands of a competitor.

This article originally appeared in *Law360* on May 2, 2017.

Related People

Lariza Pruneda Hebert
Of Counsel
713.292.5603
Email