Best Practices for Restrictive Covenant Agreements When Employees Leave

Publication
12.02.13

Risk managers have to be prepared for the unexpected. That often takes the form of being ready for external threats to a business such as a severe economic downturn or a natural disaster. Eons of experience and natural selection conditioned human beings to perceive threats from outsiders. However, risk managers must also consider the prospect of threats from within or, specifically when an insider becomes an outsider. Some employers assume their current workforce–and especially key personnel within that workforce–will remain with them forever. Many decision-makers do not think about a star performer getting a better offer from a competitor or having a falling out with her/his supervisor.

However, change is inevitable, especially in the employment arena. Employees–even those who value and exhibit loyalty–rarely spend their entire careers with one company. So what does a smart company do to prepare for the possibility that a key employee will move to a competitor? And what should a wise risk manager advise the executives at that company regarding the threat of competition from an existing employee who maintains some of that company's key relationships and knows where the proverbial skeletons are buried? Following are some best practices.

1. Have restrictive covenant agreements in place.
The best way for a company to protect itself against competition by former employees is to have restrictive covenant agreements in place. These agreements can deter employees from leaving in the first place. They also can deter competitors from hiring your key employees or, in the event that the competitor does hire a key employee, it will do so subject to restrictions on that employee's activities and job duties. If a key employee chooses to depart, then the agreements can prevent the employee from:

- competing in certain territories and/or on behalf of certain competitors;
- soliciting customers with whom the employee had a relationship;
- soliciting or hiring co-workers; and
- using or disclosing confidential information.

It is important to note, however, that state laws vary regarding the enforceability of such agreements, so work with legal counsel to determine how to structure the agreements. The mere fact that an employee agrees to certain restrictions by signing an agreement does not mean that a

fact that an employee agrees to certain restrictions by signing an agreement does not mean that a judge will actually require that the employee comply with the covenants. Moreover, there is little rhyme or reason to the states that are hostile to enforcing restrictive covenants. Some states with pro-employee legal regimes are favorable for enforcing non-compete restrictions and some are not. The opposite is also true.

For instance, certain states have rules in place that prevent the use of non-compete restrictions altogether. Other states restrict the categories of employees who can be subject to a non-compete agreement. Often, the forum where a restrictive covenant agreement is litigated and the law that is applied to the agreement will determine whether the agreement can be enforced. An employer can address that issue on the front end by specifying the forum and governing law in the agreement, but these provisions are–like non-compete paragraphs themselves–not always enforceable.

Additionally, some states have specific requirements relating to the execution of restrictive covenant agreements. For example, approximately 10 states require the provision of additional consideration (i.e. a raise or a bonus) for existing employees to sign enforceable restrictive covenants. In general, it is a good idea to consider which employees pose a potential competitive threat and then use detailed agreements with them, whereas lower-threat employees should sign shorter, less burdensome agreements.

2. Think through key information and take steps to protect it.
To stop a former employee from using or disclosing confidential information, an employer needs to show that information is truly non-public. If other employees are permitted to walk out the door with that information, then such a showing will be very difficult. Likewise, if the information is provided to third parties without safeguards in place, then the information will lose its confidential character. Thus, it is important for a risk manager to ask two questions:

1. What information would be most useful to competitors if an employee left with it?
2. If asked on a witness stand by a judge (or by a company attorney while drafting an affidavit) "How many measures does the company take to ensure that the information remains private?"

Restrictive covenant agreements can be useful for a company because they represent one means by which the company can show that it protects its proprietary information. However, the agreements have to be enforced in order for this argument to work. Additionally, the best practice for the company will be to have a general definition of confidential information and then to list the specific categories that matter the most to the company. A specific list will have an educational effect on signing employees, and it will make enforcement easier.

3. Make clear that employees cannot misuse the practice's computer system.
With the increased use of the federal Computer Fraud and Abuse Act and analogous state law computer protection statutes, employers are learning the importance of putting employees on written notice as to what they are not authorized to do on the company computer system. This includes both taking files from the system (such as by e-mailing files out as attachments or saving

them to thumb drives) and deleting files prior to departure. The key to unlocking the power of federal and state computer protection laws is showing that the employee was on notice that he was not authorized to perform certain acts on the system. Thus, a comprehensive restrictive covenant agreement should place an employee on notice as to activities that exceed authorization on the computer system.

4. Define the employer's property.
It may seem obvious that an employee is required to return employer property at the end of employment, but the question of "what does the employer truly own" can arise. For instance, what about work e-mails that an employee sends from his/her personal email account during the course of employment? When that employee leaves and moves to a competitor, the information in and attached to those emails could prove useful in competing with a former employer. Departing employees often retain those e-mails inadvertently and then find them useful after moving to a competitor. Other employees plan on using those emails from the start. In either event, putting the employee on notice as to the categories of information that he/she is required to return and delete is a worthwhile use of time.

The issue of protecting the company against the prospect of former employees competing unfairly against it is a classic example of the maxim that an ounce of prevention is worth a pound of cure. Relatively small expenditures of time and money on the front end can either deter an employee from seeking to exploit your company's key relationships and information or position the company to stop such exploitation on the part of a former employee. The critical first step is to plan for an unpleasant possibility through the use of restrictive covenant agreements.

This article by Michael Elkon was also featured on Constructionexec.com