The Legal Intelligencer
THE OLDEST LAW JOURNAL IN THE UNITED STATES 1843-2012
PHILADELPHIA, WEDNESDAY, OCTOBER 31, 2012 VOL 246 • NO. 86 An ALM Publication

The Brave New World of Noncompete Clauses

BY MARGUERITE S. WALSH
Special to the Legal

As almost any business owner can attest, the challenging economic climate has brought increased activity around the obligations of former employees. Whether an employee loses a job because of financial cutbacks or moves to another company for a better opportunity, he or she may be looking more closely than ever before for the proverbial leg up to secure, and succeed in, future employment. Unfortunately for companies, this may result in a greater tendency by departing employees to download sensitive company information and otherwise run afoul of their post-employment restrictions against solicitation and competition. According to a 2009 study by Larry Ponemon, "Data Loss Risks During Downsizing: As Employees Exit, So Does the Corporate Data," nearly 60 percent of employees who quit or were discharged acknowledged taking proprietary data from their employers.

Conversely, companies facing similar economic pressures are more likely to use every weapon in their arsenals to protect their competitive positions. However, the increasing irrelevance of geography as a meaningful limitation on a former employee's activity, the speed and methods by which confidential information can be transmitted and the many variables that already exist in the context of attempted enforcement of post-employment restrictions make it even more challenging for employers to know how best to proceed. Instead of becoming overwhelmed and possibly paralyzed with uncertainty, companies would be well-served by returning to the basics of protecting their legitimate interests, with due recognition of the changing landscape. This article provides five practical suggestions about how to do just that.

KNOW YOUR AGREEMENTS (AND WHERE THEY ARE)

Many companies, especially those with numerous divisions and affiliates, utilize what can best be described as a hodgepodge of agreements containing post-employment restrictions. This is particularly true in situations involving mergers, acquisitions and restructuring, which of course are quite common. Two key individuals performing virtually the same functions and having essentially the same potential to inflict competitive harm may be subject to two entirely different sets of restrictions, depending on the language of their agreements. Two agreements that are almost identical in terms of the substance of the post-employment restrictions may be vastly different in terms of enforceability depending on whether certain technical requirements (like consideration) have been met. On top of these differences, it is not unusual for companies to have no central repositories for their agreements or to discover that the requisite signatures have not been obtained. While companies (including their HR departments and any in-house counsel) are stretched to maximum capacity on all fronts, a periodic review of the status of post-employment agreements — at least for key personnel whose departures and misconduct are likely to cause the most competitive harm — is time well spent. Often, companies take an all-or-nothing approach to revising their agreements that becomes too daunting (and expensive) to accomplish, when a more focused, incremental approach is more realistic and can actually yield meaningful improvement.

MARGUERITE S. WALSH *is a shareholder in the Philadelphia office of Littler Mendelson. She focuses her practice on representing companies in matters involving protection of intellectual capital and customer relationships, including trade secrets and post-employment restrictions. She can be reached at 267-402-3016 and mwalsh@littler.com.*

KNOW YOUR CONFIDENTIAL INFORMATION

Too often, companies faced with potential misappropriation of proprietary information by departing employees are forced to address the situation on the fly because they do not have a firm grip on what is, and is not, considered proprietary. This in turn leads to poor decision-making regarding enforcement and disappointing results. Companies should conduct regular audits to identify and update the body of information that is considered protectable. This may include not only technical/R&D information, but also production/process, cost/pricing, quality control, financial and customer/client information. Consult with those employees having the most relevant knowledge of the information in question, who can speak to the reasons why it should be protected. Ideally, create lists of such information within each business unit or department as well as a master list, along with an identification of those employees who have access to it. Update the lists on a regular basis. Again, this may be a daunting task for many companies given limited time and resources, but it is worthwhile to at least focus on the types of information and/or business lines where the risk is greatest.

It is not enough for a company simply to identify what information constitutes trade secrets or proprietary information; it must also demonstrate that it takes reasonable steps to maintain the secrecy of the information in question. While much has changed (and keeps changing) with regard to technological advances that make it challenging for companies to police access to proprietary information, companies should keep in mind that the good old-fashioned ways of restricting access to confidential information are still viable and valuable. These may include: stamping and labeling (including electronic labeling) documents that are considered confidential; using sign-in logs at company facilities; preventing visitors from wandering unescorted on company premises; shredding or otherwise destroying hard copies of proprietary information; maintaining physical barriers to access when appropriate; using and

updating proper password protection; using appropriate monitoring software; including a policy in the handbook concerning access to confidential information; including in job descriptions relevant language for employees who have access to proprietary information; and using nondisclosure agreements. If enforcement efforts are required, consistent adherence to these sorts of practices can be of great assistance.

KNOW HOW TO DEAL WITH THE BYOD MOVEMENT

In just the past few years, as the line between work and nonwork activities continues to blur, companies have encountered a trend that radically alters the way people perform their jobs. The exploding usage of personal devices for both work and nonwork purposes (known as the Bring Your Own Device, or BYOD, movement) presents employers with a new and often uncharted set of challenges. This is particularly true in the case of protection of confidential information and other post-employment obligations. Whereas previously a company simply fired an employee who was found storing or copying company data onto a personal device, if the company not only allows but encourages such behavior, that response is no longer automatically the appropriate one. Moreover, a recent study by the Ponemon Institute on mobility risks shows that companies are often unaware whether and what kind of data might be leaving their networks via nonsecure mobile devices.

The most conservative approach to managing the task of protecting proprietary information is to eliminate the use of nonsecure mobile devices from the workplace entirely, or at least in instances involving individuals with access to the information the company considers proprietary. A company may decide to purchase company-owned devices for such individuals, requiring them to be used only for company purposes, which, at least theoretically, gives the company some greater level of control over the devices themselves and the data they contain.

Many companies, however, already sanction dual-usage devices, so the question becomes one of balancing and finding the best mix of practices to address the realities of the work situation and the need to maintain confidentiality. Steps might include: company ownership of the device (for the reasons noted above); more focused attention on confidentiality agreements and training around the need to maintain confidentiality; limitations on (or prohibition against) the use of cloud-based storage for proprietary information; strong emphasis on mobile device safety and strict adherence to reporting requirements for lost or stolen devices; and the use of MDM (mobile device management) software that allows companies to remotely manage and configure many aspects of dual-use devices.

USE EXIT INTERVIEWS AND REMINDER LETTERS

The exit interview is a simple, yet often overlooked, tool to minimize the loss of proprietary information and/or clients when an employee leaves. While exit interviews are common, they often do not focus sufficiently on the departing employee's post-employment obligations. An employee will announce an intention to depart to pursue unspecified "other opportunities" and then, weeks or months later, the company learns of wrongdoing that can pose a significant business risk. While an effective interview may not prevent the conduct from occurring, it could provide helpful evidence in support of enforcement actions and can often reduce risk. At a minimum, have all relevant documents relating to the employee's post-employment obligations in hand for the interview; remind the employee of those obligations; address the return of company property and of the employee's personal property; try to ascertain the employee's future plans; and consider having the employee sign an acknowledgment of his or her continuing obligations.

Many companies, especially those with numerous divisions and affiliates, utilize what can best be described as a hodgepodge of agreements containing post-employment restrictions.

Many companies also have a regular practice of reminding former employees (and often their new employers) in writing of any post-employment obligations that may exist, even in situations where there is no suspected wrongdoing. This is a beneficial practice for at least four reasons.

First, if wrongdoing does occur, such a reminder can serve as helpful evidence of the company's active steps to protect its interests in the situation at hand. Second, even in the absence of wrongdoing by the employee in question, it can be helpful in other cases to show that the company takes regular steps to protect its interests. Third, it helps reinforce a culture of compliance within the company. Fourth, including the new employer in the correspondence places it on notice of its new employee's post-employment obligations. These reminder letters need not be accusatory or confrontational (and in fact need to be especially carefully drafted when the new employer is copied or included to avoid potential defamation or tortious interference issues). They can simply enclose the relevant agreements, remind the former employee of his or her obligations and ask for information regarding specific steps the former employee (and the new employer) are taking to ensure compliance.

KEEP YOUR OWN (HIRING) HOUSE IN ORDER

No matter how proactively a company might act to safeguard its legitimate interests in its proprietary information, client relationships and good will, all its efforts can become meaningless (and, worse, backfire) if it does not engage in the same type of prudent behavior when hiring employees from competitors. Sound practice in the area of noncompetes and confidential information is a two-way street and a company should act carefully and responsibly whether pursuing its own rights or considering those of a new employee's former employer. •