Published on *The National Law Review* https://natlawreview.com

Developing Plan for Employee Departures in California

Article By:

Peter A. Steinmeyer

As discussed prevously in Critical Importance of Realistically Identifying and Protecting Trade Secrets and Confidential Information, although California employers generally cannot restrict an employee's ability to work elsewhere, California employers can protect their trade secrets and confidential information. One pillar of a successful plan to do so is having an employee departure protocol.

The foundation of a solid employee departure protocol is the exit interview. Employers should know *who* will conduct it, *when* it will be held, and *what* will be covered.

There should be a written checklist for the exit interview, and it should cover threshold topics, such as reminding the departing employee of his or her continuing confidentiality obligations, the return of company property and information stored on-site (e.g., access cards, laptops, and iPhones), and arrangements for the return and/or destruction of company property stored off-site.

The discussion of possible company property stored off-site should cover specific locations that a departing employee might not think of unless specifically asked, including thumb drives, personally owned computers, and personal email or cloud storage accounts. Many a lawsuit has been filed over forgotten thumb drives in employee backpacks.

The departing employee should also be asked to sign a certification that he or she has or will return all of the employer's property by a date certain, and someone needs to follow up to make sure this is done. The signing of such a certification reiterates the importance of the employee's confidentiality obligation. Additionally, should that certification later prove false (i.e., if it is later determined that the employee, in fact, misappropriated trade secrets), the false certification will be a critical piece of evidence in showing the reasonableness of the employer's efforts to protect itself—and maliciousness by the former employee.

If an employee is departing under suspicious circumstances, or if there is other reason to suspect possible misappropriation of trade secrets, records of the employee's computer activity in the days and weeks leading up to his or her termination should be preserved (e.g., by saving the employee's e-mails and making a forensic image of the employee's hard drive, rather than simply wiping it and reissuing it). Litigation over trade secret misappropriation frequently turns on evidence of unusual computer activity shortly before a departure. The employer should have a plan for accomplishing this, whether it be an internal resource, such as its information technology department, or an outside

forensic computer firm.

Finally, depending on the facts of a particular situation, a formal “cease and desist” letter to a departed employee and/or a less threatening “reminder” letter can be a valuable tool. Such letters can come from the human resources or legal department, and not only serve as useful written reminders to the departed employee, but may also resolve a dispute without proceeding to litigation. Depending on the situation, an employer may also decide to send a copy of the “cease and desist” or reminder letter to the employee’s new employer.

In conclusion, different employers have different needs with respect to the protection of their trade secrets and confidential information, and reasonable precautions for one employer might be completely unreasonable for another. However, regardless of the size or nature of the business, every employer should develop and maintain an employee departure protocol.

National Law Review, Volume VII, Number 136