

HOW TO PREVENT THE THEFT OF YOUR CLIENTS

Scenario. *On Friday afternoon, at 4:43 p.m., your office manager drops a bomb: she is quitting to work for "Acme Staffing," a tough competitor that has just opened an office in your primary territory, and two lower level office personnel are leaving with her. By Monday afternoon some of your best clients call to tell you they have received solicitation letters from her asking them to use Acme for their staffing needs. The solicitation letter indicates that Acme is aware of their unique staffing needs and requirements, and that Acme can offer new competitive pricing. You also learn, after contacting your core-client base, that Acme has sent similar solicitation letters to every customer in your computer database. Lastly, you discover that your departing employees took their rolodexes and copied several key customer files, as well as information relating to your pricing structure, computer data, and historical customer information.*

Ten years of hard work will be lost if you can't stop her. Can you?

If you have adequately prepared for this scenario, you can prevent a wholesale pirating of your clients and your valuable client information. Indeed, if you follow the simple steps outlined below, you may be able to obtain an injunction, within *hours*, preventing your former employees and their new employer, from (1) contacting your clients; (2) accepting business from clients they have already wrongfully solicited; and (3) using any of your proprietary customer information. You may also later seek money damages for your former employees' and competitors' illegal practices. Similarly, failure to prepare for this scenario may prevent you from obtaining *any* meaningful relief, or, may delay relief sufficiently that your client base is irreparably damaged.

What can you do? The following measures are critical to protect your customer base, and to create an office culture that will ensure that your employees, from the

managerial level to the lower staffing levels, understand their contractual and common law duties to your company.

STEP NO. 1 Compile each and every employment agreement for your current employees for review by legal counsel. As is often the case, employment agreements evolve over time, such that there may be great discrepancies between employees who were hired several years ago with the agreements signed by recently hired employees.



As part of every employment agreement, at a minimum, there should be provisions providing for the employee's fiduciary duty to his or her employer, and provisions providing for acknowledgment of the confidential nature of your customer information (including information that may be learned by the employee over the course of their employment). The agreements should further reflect that employees acknowledge that irreparable harm would be caused if customer information is misappropriated and agree to immediate injunctive relief for their failure to abide by their duties upon termination. (In this regard, it is often advisable for the employment agreements to indi-

cate both what state law should be applied to interpret and enforce the provisions of the employee's contract as well as whether State court or Federal court or other arbitration mechanism is preferable by the employer.)

These various contractual provisions may often be incorporated into separate agreements (Employment Contracts, Covenants Not To Compete, Agreements of Confidentiality, Non-Disclosure Agreements, etc.). Moreover, where these provisions are not currently contained in employee contracts, caution must be advised when supplementing employment agreements. In many states, certain amendments to employment agreements (especially those containing non-compete provisions) may be unenforceable unless accompanied by *some* consideration, such as a bonus, increased pay, change in title and responsibility, and the like. In this respect, reference to your specific state laws where your employees are working is strongly suggested when making this determination.

STEP NO. 2 An analysis should be performed of any existing contracts or contractual provisions providing for restraints on competition, sometimes referred to as "covenants not to compete" or "restrictive covenants." The law relating to the enforceability of these covenants has evolved rapidly over the last several years and, in many cases, has limited the allowable scope, both geographic and time limitations, that can be imposed upon an employee upon their resignation or termination. Indeed, the failure of a restrictive covenant to accurately reflect the current limitations imposed by State law may lead to a complete inability to enforce the restrictive covenant at all. In this respect, if an employee's restrictive covenant was drafted in a manner that is no longer consistent with current State law, it may be possible for such an employee to actively compete upon their resignation even if

compensation was paid to that employee for their agreement not to compete.

STEP NO. 3 Attention must be focused on office procedures for maintaining the confidential and proprietary nature of your customer information. In this respect, many employers make the serious mistake of requiring their employees to sign agreements regarding confidentiality without implementing measures to protect that information. The failure to do so may lead to legal difficulty in enforcing confidentiality agreements. These procedures may be as simple as password-protecting computers, not giving client lists and other customer information to non-employees, and requiring that employees sign out hard copy files when removing customer files from storage.

CONCLUSION If these moderate steps have been taken, you may be able to prevent a theft of your client base if a similar scenario, as described in the opening of this article, should occur in your office. However, without advanced preparation, including review of your current employee contracts, the time in which it may take to obtain meaningful relief may turn from several hours to several weeks or, alternatively, may prevent you from obtaining any relief at all. In this regard, a small investment in time and resources can prevent the irreparable harm that often accompanies departing employees who attempts to pirate your clients. Experience has further shown that employers who seriously pursue these policies, both through internal procedures and through quick and decisive action, can often prevent theft of their clients by creating a culture which discourages acts of unfair competition both on the part of employees and competitors. In summary, the process of protecting your customer base and proprietary information is simple and inexpensive compared to the cost of failing to prepare for employees and competitors bent on stealing your clients. ■

Jon D. Cohen is an attorney with Ungaretti & Harris of Chicago where he handles employment and trade secret litigation. He can be reached at (312) 977-4123.

EMPLOYMENT DOCUMENTATION CHANGES

On January 30 of this year, the Immigration and Naturalization Service, under a mandate to revise its employment verification procedures by reducing the number of acceptable documents, published new "proposed rules" which will become final after a period of time for comments from employers and the public.

Under the proposed new rule, the following would be acceptable to establish both a new hire's **identity and employment eligibility**:

- US passports;
- permanent resident cards;
- alien registration receipt cards;
- temporary resident cards;
- employment authorization documents;
- foreign passports with the proper temporary stamps; or
- foreign passports with proper authorization documents in those cases in which an alien is authorized to work only for a specific employer.

Documents approved to establish identity only:

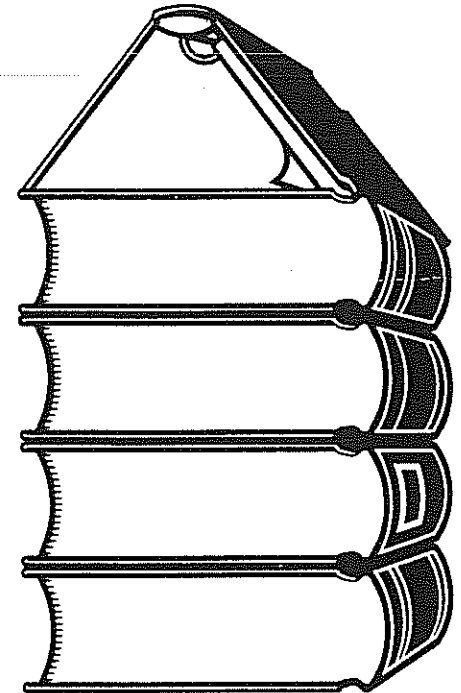
- drivers' licenses issued by a state or outlying possession;
- identification cards issued by a state or outlying possession;
- Native American tribal documents; and
- drivers' licenses or identification cards with photographs issued by Canada to Canadians authorized to work only for a specific employer.

Documents establishing employment eligibility only:

- social security account numbers without employment restrictions;
- Native American tribal documents; or
- proper forms establishing that an alien is authorized to work for a specific employer.

Identification documents no longer eligible:

- identification cards issued by federal or local authorities;
- school identification cards;



- voter registration cards;
- military dependents' identification cards;
- merchant marine cards;
- for those under 18, school records, report cards, day care or nursery school records, and clinic or doctor records.

Employment eligibility documents removed:

- state department certificates of birth abroad;
- birth certificates issued by a state, county, municipal authority, or outlying US possession;
- identification cards for resident US citizens;
- documents that are not permissible for both identity and employment eligibility.

Congress has removed birth certificates from the list of acceptable documents out of concern that they might not belong to the person who presents them. The text of the proposed rule and drafts of the new INS forms are available at the INS web site at www.ins.us.doj.gov. ■