Maintaining Trade Secret Status For Customer Lists: Five Steps Every Company Can Take to Protect Customer Information

Insights
10.07.10

Many employers consider their customer list to be a trade secret. As this blog has previously noted, 46 states plus the District of Columbia have enacted a version of the Uniform Trade Secrets Act. In some states, the statute goes so far as to expressly provide that a customer list may qualify for trade secret protection. For example, in Colorado, a trade secret may include "names, addresses or telephone numbers, or other information relating to any business or profession which is secret and of value." See Colo. Rev. Stat. Ann. § 7-74-102(4). Other states are more generic and do not expressly mention customer lists. Rather, generally speaking, a trade secret is a (1) compilation of information, (2) that derives independent economic value to the owner, (3) because it is not generally known or easily ascertained by others through proper means. It is important to note, however, that trade secret status is not automatic in any state. Stated differently, although a customer list may qualify for trade secret protection, the trade secret owner will bear the burden of showing that the information is in fact a secret and valuable.

There is no magic "formula" for achieving trade secret status for a customer list, but there are many different steps a company can take to improve its odds. Here are five:

1. Establish Ownership. Contractual clarity is helpful. Employment agreements should require employees to acknowledge that customer records and information, specifically including their identities and other data about their preferences, contact information and the like belong solely to the employer and are considered to be the company's trade secrets. This may even mean taking steps to ensure customer information is not disclosed through social media such as LinkedIn, Facebook or Twitter.

2. Prohibit Misuse Through Nondisclosure Agreements. Employment agreements should contain nondisclosure agreements with language stating that employees may not use or disclose customer information except for the sole purpose of conducting business on behalf of the employer.

3. Maintain Computer Security. Customer information should be protected in all forms, including on computers. Maintaining a secure computer system is not a simple task, but the following steps should be considered: require passwords; limit employee access to certain information on a need-to-know basis; implement controls on what can be downloaded; make sure your system has all of the latest security patches and fixes installed; and if the company's system is on the internet, use a firewall and routinely audit servers for security gaps.

firewall and routinely audit servers for security gaps.

4. Remind Employees. Don't let employees forget that your customer information is company property and may not be disclosed. Flag computer systems with messages and dialog boxes with reminders. Include confidentiality language in policy manuals and handbooks. Send written reminders in annual compliance or business practice updates. Remind employees during meetings and review sessions. Periodic emails can be used. In short, take advantage of natural opportunities to remind employees.

5. Limit Access. In addition to protecting computer systems, carefully monitor and limit access to customer files. Do not store customer records in areas that are accessible to the public or to all employees. Limit employee access to information only about the customers they personally service.

For more details on protecting your trade secrets, see our prior post regarding implementing a trade secrets protection program. And as always, please feel free to let us know your thoughts and questions in the comment section below.

Related People

Michael R. Greco
Regional Managing Partner
303.218.3655
Email