

Top Ten Non-Compete and Trade Secret Concerns for Inhouse Lawyers and the Companies They Represent

Insights
12.06.10



Protecting a company's non-compete and trade secret interests can be a daunting task. There are so many things to consider. Here's a list of ten things to keep in mind and some resources to help you take action.

1. Implementing a Trade Secrets Protection Program -- Protecting your trade secrets cannot be left to afterthought. Companies are well advised to implement a trade secrets protection program. If you don't know where to start, consider conducting an audit of your company's confidential information.
2. Drafting Non-Competition Agreements -- Many employers with offices or employees located in multiple states use the same non-compete/confidentiality agreement in each state in which they do business. Typically, the form of the non-compete/confidentiality agreement originated in the employer's home state, and the employer went on to use this same agreement wherever the employer does business. However, these employers may find out too late that a non-compete/confidentiality agreement enforceable in their home state may not be enforceable in another state.
3. Online Social Networking Policies -- Chances are that one-quarter to perhaps as much as one-half of your workforce (or more if your workforce is younger) are regular users of social networking websites. Any business that does not have a social networking policy or does not train its employees on the do's and don'ts of social networking may have a critical security gap in the protection of its trade secrets. A recent case suggests that LinkedIn can present a threat to your trade secrets. If you have expectations concerning the manner in which your employees may

or may not use LinkedIn, it is wise to address these concerns upfront through contracts and written policies.

4. Can Your Lawyer Keep a (Trade) Secret? -- Ensuring that your trade secrets are kept secret is not a new requirement. Internal controls on use and dissemination of confidential information may not be entirely sufficient. Businesses need to recognize that risks sometimes involve the handling of their data by third parties specifically entrusted for that purpose, such as their attorneys. Remote storage of client data presents several concerns including unauthorized access to confidential client information by a vendor's employees or by hackers, a failure to adequately back up data, or insufficient data encryption.
5. Can Litigation Place Trade Secrets at Risk? -- The last place you might expect your trade secrets to be at risk of disclosure is in a court action intended to protect them, but courts around the country have held that plaintiffs alleging trade secret misappropriation must identify the secrets at issue with specificity. So what is a plaintiff to do if it wishes to minimize disclosure of its trade secrets during litigation while maximizing its ability to discover what information may have been taken by the defendants?
6. Open Source – Hidden Exposure -- Open source code is computer code that is publicly available on the internet for use by anyone. Typically, in order to copy open source code from the internet, a party must agree to the terms of a "click" or similar pop-up license. Although there are hundreds of different open source code licenses, many require that the user of the code must make publicly available any subsequent use of the code. In other words, if your software programs are built using open source code, it may be more difficult to claim trade secrecy for such programs.
7. Taking Control of Litigation Budgets in Non-Compete Cases -- Litigation budgets can be difficult to prepare under the best of circumstances. Budgeting for non-compete litigation, with its unpredictable nature and often front-loaded cost structure, is even more difficult. Although many factors are outside the control of parties and their counsel when it comes to litigation costs, the litigation strategy you choose can have a particularly significant impact on your budget in a non-compete case. Moreover, given the fast pace of non-compete litigation, there is an increased need to continually reassess your budget early on as developments unfold.
8. Handling Employee Defections -- When employees leave to join a competitor, you can often be taken by surprise. In order to secure your confidential information and customer relationships, rapid action may be required. Consider these ten tips for responding to employee defections.
9. Advising Recruits -- Just as employers must be prepared to respond to employee defections, they must be prepared to advise their incoming recruits on what not to do when resigning from a former employer. Here are ten things to keep in mind.
10. Mergers and Acquisitions -- Good mergers can turn bad without attention to employee retention -- be sure to carefully analyze the existence and enforceability of non-competes signed by key employees early in the process.

Michael R. Greco is a partner in the Employee Defection & Trade Secrets Practice Group at Fisher Phillips. To receive notice of future blog posts either follow [Michael R. Greco on Twitter](#) or on [LinkedIn](#) or subscribe to this blog's RSS feed.

Related People



Michael R. Greco
Regional Managing Partner
303.218.3655
Email