LinkedIn: A Violation of Your Employee's Non-Compete?

Insights
10.03.10

A sales manager has signed a contract with his employer agreeing that client lists are confidential and agreeing not to solicit clients for a period of six months after the end of his employment. Shortly after resigning to join a competitor, the sales manager updates his LinkedIn profile to reflect that he has changed jobs and is now working for the competitor. The profile update is broadcasted by LinkedIn to the sales manager's contacts, which includes dozens of the clients he serviced at his previous employer. Has the sales manager breached his contract? Arguments can be made on both sides.

The former employer will argue that its customer list is confidential and that the sales manager obtained his knowledge of the clients' identities by virtue of his employment. The employer will note that even novices on LinkedIn understand that the service will notify contacts of a user's profile updates. After all, why bother updating your profile if you don't intend to share this information with others? And many, though admittedly not all, courts have held that contacting former clients regarding a change in employment constitutes a solicitation. See e.g., Merrill Lynch v. Schultz, 2001 WL 1681973, *3 (D.D.C. 2001) (noting that "such initiated, targeted contact is tantamount to solicitation because there is no reason to believe that a customer on the receiving end of such a [communication] does not assume that the [employee] wishes for him to transfer his account.").

The sales manager will undoubtedly take a different view. He will argue that he didn't take any records or other information with him when he left, and that the identity of his former employer's clients has always been publicly available to anyone who wanted to look at the sales manager's LinkedIn contacts. He will also note that he did not initiate contact with clients. Rather, all he did was update his profile to reflect a change in employment and sat back providing clients – or anyone else for that matter – with the option to contact him.

So who is right? As with any non-compete case, the answer may vary on a case by case basis and require a close examination of the contract language and the surrounding facts and circumstances. A court is likely to ask the following questions (among others): Does the contract specify that client information (such as client identities, names, addresses, and other contact information) is confidential? Did the former employer actually treat such information as confidential? What is the wording of the non-solicitation agreement?

Because the enforceability of a restrictive covenant is highly discretionary in many states, employers who seek to preclude employees from contacting clients via LinkedIn may take steps ahead of time

who seek to preclude employees from contacting clients via LinkedIn may take steps ahead of time to eliminate any confusion. Such steps may include any or all of the following:

1. Draft non-solicitation agreements that:

- expressly preclude employees from contacting clients to notify them of the employee's change in employment;
- specify that communications made through an online social networking website such as LinkedIn, Facebook, etc. constitute a violation of the contract.

2. Draft confidentiality agreements that:

- expressly define confidential information to include client identities and contact information;
- unambiguously state that confidential information may not be used or disclosed for any purpose other than on behalf of the employer, including through social media.

3. Include a social media paragraph in non-competes that specifically addresses the use of computers and social media. The paragraph should state that:

- It is not intended to limit the scope of the confidentiality and non-solicitation covenants;
- Employees may only use the employer's computer systems (e.g., computers, internet, servers, internal e-mail, external e-mail, World Wide Web access, etc.) for business purposes only. Recognizing the rigid – perhaps impractical nature of this restriction – the agreement may provide that incidental personal use of computer systems is permitted, but state that such usage shall not violate the terms contained the confidentiality and non-solicitation provisions;
- All e-mail and internet usage is subject to monitoring and that access to any website on the Internet must be for legitimate business only;
- The Employer may choose to block access to certain sites on the Internet at its discretion, and that available access to a site does not constitute approval to use or access that site by the employer.
- The employee is not permitted to have a webpage or website on the Internet for business purposes through a provider without prior written approval from the employer. This includes social networking sites like Linked-In for business purposes. The employee should agree that mentioning his or her affiliation or employment with the employer on these types of sites without prior written approval of the content by the employer is not permitted. If the employee is permitted to connect with clients via LinkedIn, they should be required to set their settings so that other users cannot see their contacts.
- The employee agrees that the use of text messages, e-mails, IM's, and/or other communications via Blackberry or other wireless service/devices not routed through the employer's systems is not permitted for business communications with Clients;

- The employee agrees that participation in chat rooms or other online forums for business purposes is not permitted, and that the employee will not direct Clients to chat rooms, blog sites, or other social networking sites which contain information prohibited by the employer or applicable regulatory authorities;
- The employee agrees that he or she will not discuss the employer, its business relationships, its managers and employees, its customers or its products/services in any chat room or other online forum without prior express written permission from the employer's management;
- The employee agrees that the restrictions outlined above apply to his or her use of any computer (within or outside of the employer) for any business purpose.

In short, businesses that do not address social networking through their contracts and written policies may find that they have a critical security gap in the protection of their trade secrets and customer relationships.

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