Say What?

Terminated employees 'own' their LinkedIn accounts (and the company's trade secrets)?

Companies are getting a big surprise these days: Employees are leaving with their LinkedIn accounts and the company's proprietary list of business contacts. LinkedIn is a well-known, business-oriented social media website that allows account holders to add business contacts and develop a network. Companies are mistakenly lettting employees add the firms' business contact lists to employees' LinkedIn accounts.

This can result in the company losing trade secret protection for its business contact lists in several ways.

First, without a social media policy, the company may unknowingly give the employee ownership of the company's confidential business contact lists.

Second, LinkedIn may reveal an employee's "contacts" to the public, thereby allowing an employee to add business contacts to the employees' LinkedIn accounts without rules on maintaining confidentiality. This may result in a loss of a big proprietary business asset and a trade secret because this can be used as proof that the company made no effort to keep that trade secret "secret."

> Without a social media policy, the company may unknowingly give the employee ownership of the company's confidential business contact lists.

Third, "password-protection legislation," which prohibits employers from requesting or requiring that employees disclose social media log-in credentials, may affect their ability to claim their proprietary company business contacts. In some states, employers can no longer force employees to disclose the passwords to their Linked-In accounts. The law has already been enacted in seven states: Maryland, California, Illinois, Michigan, New Jersey, New Mexico and Utah. And the law is pending in more than 20 state legislatures, so the legal landscape undoubtedly will become more complex over the next one to two years, especially for multistate employers.

If your company does not have a clear social media policy and an employment agreement that establishes ownership of the employee's LinkedIn account, the employee may have the right to walk out with all of your business contact information (trade secrets). You need to fix this problem now.

Without a social media policy, courts may conclude your employee "owns" the LinkedIn account and your business contact information (trade secrets). A 2013 Pennsylvania court in Eagle v. Morgan concluded that the employee, not the company, owned the LinkedIn account. The company encouraged employees to create and use LinkedIn accounts, but it never established clear policies that the company owned these LinkedIn accounts or how the LinkedIn accounts should be set up so that business contacts were not disclosed to the public. Employees then added the company's business contacts to their LinkedIn accounts.

After CEO Linda Eagle was terminated, the company (Edcomm) allegedly changed the password on her LinkedIn account, which thereby prevented her from accessing LinkedIn, then replaced her name and photo with that of the new CEO, Sandy Morgan. These facts enabled Eagle to successfully prove her claims of invasion of privacy by misappropriation of identity and unauthorized use of her name in violation of Pennsylvania law. Edcomm's claim that Eagle stole the company's business contacts was denied because there was no evidence that Eagle's contacts were developed through an investment of company time and money, as opposed to her own time and past experience.

What employers need to do now:

1. Employee agreements and policies should establish who owns the company's social media account, which is key in such disputes, as it determines who actually owns the account.
2. The company should register or create the LinkedIn account.
3. The company should specify a procedure for returning log-in information upon termination.
4. At termination, employees must be reminded of these employment agreements and policies, and employers should ensure that they obtain the relevant usernames and passwords from the terminated employee.
5. Employers should immediately change the password at the employee's termination to avoid confusion.

Without the above policies and agreements set in place, companies should not change passwords or add new photos to the terminated employee's account, as that type of conduct may expose the company to other legal violations.

These "best practices" can help an employer protect trade secrets; however, employers are advised to consult with experienced legal counsel to ensure that they are in compliance with the law.

D. MICHAEL REILLY, a shareholder at Lane Powell and director of the firm's Labor and Employment and Employee Benefits Practice Group, represents small and large employers in all facets of employment-related issues and litigation. He can be reached at reillym@lanepowell.com or 206.223.7051.