$1.50 VOL. 38 NO. 24 www.ocbj.com JUNE 15-21, 2015

ORANGE COUNTY BUSINESS JOURNAL

Stuart Kane LLP

Using Social Media Policies to Protect Your Proprietary Customer Information

by Peter Wucetich, Partner, Stuart Kane LLP

Many companies are investing increased time and resources making sure their key employees have a presence on all the relevant social media platforms, but what happens when those key employees leave? Their connections, friends, and followers resemble a de facto customer/target list, and their social media account provides a built-in way to communicate with everyone on that list at the touch of a button.

If you do not have a sufficient social media policy in place, the departing employee might be able to leave and take their social media accounts, including all contacts and content, with them when they go.

In a recent case, an employee with a company-based Twitter account had grown to over 17,000 followers left his employer. Upon leaving the company the employee changed the Twitter handle and took the account, and its followers, with him. Since the employer did not have a social media policy in place establishing that it owned the Twitter account, the employer was left arguing that, by taking the account, the employee had misappropriated its trade secrets that the employer had not bothered to protect in a contract and that were, to some extent, available to the public. This is a weak position that could have been avoided.

However, it is a tall order to successfully establish that anything on social media constitutes a trade secret. First, the *content needs to be "secret"* in order to qualify for protection as a trade secret. It is going to be difficult to convince a court that information that is made available to all of your online connections, friends, and followers — and whoever they grant access to their accounts — constitutes a secret.

Second, you have to show that you have taken *reasonable precautions to maintain the confidentiality* of the secret. If you do not have a social media policy in place, it can be argued that you did not take reasonable precautions to protect the secret.

Additionally, a California statute creates some hurdles to obtaining login information for employees' social media accounts if the accounts were used for personal matters. California Labor Code § 980 prohibits an employer from requiring that employees disclose the username or password for the purpose of accessing their personal social media. As such, an employer needs to have a social media policy that requires that work related social media accounts be used for work purposes only, and not include personal material. If personal matters are allowed to be included as part of the mix, the employer might be unable to get the login information from the departing employee.

Employers can avoid many of these headaches by adopting a social media policy that gives them a contractual right to any work related accounts and content. The policy should make it clear that the employee is to use the account for business purposes only and require that the employee provide you with the login information when the account is created.

By adopting a legally sound social media policy, employers can create a contractual right to the account and work related content, and avoid certain burdens to prove that the account belongs to the employer or contains the employer's intellectual property.

Peter Wucetich

Peter Wucetich is a partner with Stuart Kane LLP where he focuses his practice on employment and business litigation. He routinely handles employment litigation, including trade secret misappropriation, wrongful termination and class actions. In addition, he provides employment counseling on issues relating to employee mobility, non-competition and non-solicitation agreements, and the protection and assignment of intellectual property rights developed during the course of employment. Mr. Wucetich can be reached at 949.791.5174 or pwucetich@stuartkane.com.