HOGE · FENTON

LEGAL UPDATE: PROTECTING YOUR COMPANY'S TRADE SECRETS

The ringing in of a new year often brings employee departures. And with those departures – whether voluntary or otherwise – comes the risk of loss of the employer's trade secrets.

For some employees, the new year represents an opportunity to start fresh with a new job. Some have been waiting for their year-end bonuses to make their move. Whatever the reason, do you know where your departing employees are going, and what they might be taking with them? Are they starting their own competing business? Are they joining a competitor? You may not know until it is too late — which is why you should have a plan in place to protect your business, by making sure your trade secrets and other proprietary information do not walk out the door with your departing employees.

But, I'm not sure my business even has any "trade secrets." Trade secrets can exist in any business, and are among a company's greatest assets because they provide it with a competitive advantage against others in the same industry. A business automatically owns a trade secret by: (1) creating any information, "including a formula, pattern, compilation, program, device, method, technique, or process," that has economic value to the company because it is not known to others, and (2) taking reasonable steps to keep that information secret. (**Click here** for examples of trade secrets, and for information on conducting trade secret audits.)

A company is entitled to legal protection over its trade secrets without having to register them with a government agency (unlike patents and other types of intellectual property), and that protection never expires until or unless the trade secrets are no longer secret. And there is the rub. Trade secrets can be extremely vulnerable to theft and disclosure, particularly by employees who have direct and daily access to the company's crown jewels.

What can I do to protect my business? Some of the common modes of trade secret theft by employees are: simply walking out the door with hard copy documents in hand, copying data onto electronic storage devices, forwarding documents to a personal email address, and downloading company data through remote network access after hours. A thoughtful employer can better protect itself by including a few simple security measures in its employee exiting process, such as:

- securing the departing employee's computer media
- cutting off the employee's network access
- reminding the employee of his ongoing confidentiality obligations

- requesting new employer information
- obtaining an exit certification regarding the non-retention of company data
- possibly forensically inspecting the employee's computer (computer forensics sound scary, but can cost less than one might think and often yield evidence of theft that is worth its weight in gold)

This list is certainly not exhaustive, and appropriate measures will depend on the type of business and the position of the departing employee.

For more advice regarding this or any other employment or intellectual property-related question, please contact **Sarju Naran**.

For more information on Hoge Fenton's employment law practice, please **click here**.

Primary Contact

- Sarju A. Naran

Related Attorneys

- Ashlee N. Cherry
- Jenn Protas