HOGE FENTON
Hoge Fenton Jones & Appel
Attorneys at Law | Founded in 1952

Trade Secret Audits

Many companies assume they have no trade secrets, and that trade secrets only relate to engineering and formulas. While it is true that the source code for a software application might be a trade secret, and the recipe for Coca-Cola Classic® (which is kept in a locked vault) is arguably the most famous trade secret of all, trade secrets come in several less obvious forms and can exist in nearly any business. In reality, *most* companies have actual or potential trade secrets, but they may not realize it.

What is a trade secret? A "trade secret" is defined as *anything* that has economic value (*i.e.,* gives you a competitive advantage in the marketplace) because it is kept secret. The following are just a few examples of information that might be considered legally protected trade secrets:

- Customer preferences
- Marketing/branding plans
- Sales techniques
- Negotiated pricing/contracts
- Training programs
- Financial data
- Algorithms
- Negative knowledge (what a company knows does *not* work)
- Employee strengths/weaknesses
- Profit margins
- Internal development strategies
- Lesson plans
- Metrics/analytics
- Recipes
- Product "roadmaps"
- Manufacturing processes

A company is legally protected from having anyone in the world steal, access, use, disclose, or otherwise improperly benefit from its trade secrets without the company's permission — as long as it takes reasonable steps to maintain their secrecy.

Of course, if a company wants to keep its trade secrets confidential, it helps to first know what its trade secrets are. That is why it is important for businesses to conduct regular trade secret audits, to (1) identify the company's trade secrets, and (2) identify all measures the company currently takes, and others it should take, to protect the confidential nature of its trade secrets.

Step 1: Identify Your Trade Secrets. Here are a few tips that will help a company in the first part of a trade secret audit—identifying and taking inventory of the company's potential trade secrets:

1. What gives your business a competitive advantage over others in the same line of business? Perform a thoughtful evaluation.
2. Is there information about your business that your company does not share and would not want anyone outside the company to know, because the information could help competitors and/or hurt the company? Identify this information.
3. Meet with the department heads within the organization (*e.g.,* Human Resources, IT, Finance, Sales, Marketing, Engineering, Research & Development, Product Management, Manufacturing, Legal, etc.) to determine what valuable and competitive information each department might have.
4. Consider what steps your company might take to identify new trade secrets going forward.

5. Consult with legal counsel regarding the types of trade secrets that typically exist in your industry, and engage counsel to assist in determining what specific trade secrets might exist in your particular company.

Step 2: Implement Protective Measures. Once a company identifies its trade secrets, it needs to assess what measures it already takes to protect its trade secrets, and what additional steps can be taken. With the increasing prevalence of cell phones, PDAs, flash drives, netbooks, and iPads in the workplace—not to mention the new and exciting (or scary) world of "cloud computing"—companies face new challenges every day in determining how to adequately protect their confidential information from disclosure.

While every industry and each business is unique, the following are some important safeguards companies can employ to protect their trade secrets from unauthorized access, use, and disclosure:

1. Create a written log of the functions within the company where employees have access to particular trade secrets by virtue of their job duties (do not overlook secretarial and other administrative employees who might have access because they support employees with a direct need to access trade secrets).
2. Require all employees who have or will have access to trade secret information to sign a confidentiality agreement that identifies the company's categories of trade secrets and specifies the employees' confidentiality obligations both during and post-employment.
3. Distribute an employee handbook that includes a confidentiality provision and reminds employees of their obligations.
4. Require independent contractors, vendors, suppliers, licensees, business partners, investors, prospective purchasers, and other third parties to execute non-disclosure agreements before they are given access to sensitive information.
5. Implement password protection for all company computer media, as well as all personal laptops, cell phones and PDAs, and other storage media on which employees may perform work for the company and on which trade secrets may be stored.
6. Use encryption keys for internal email communications and for sensitive external emails.
7. Store trade secret information on separate and secure drives/ servers, to prevent access by employees who have no legitimate need for the data.
8. Label sensitive documents as "Confidential" or "Trade Secret."
9. Conduct exit interviews of departing employees to remind them of their ongoing confidentiality obligations.
10. Require all departing employees who have had access to trade secrets to sign termination certifications confirming that they are no longer in possession of any trade secrets.
11. Immediately change passwords and cut off remote network access for departing employees.
12. Secure access to the company's building with key cards, front desk security, identification badges, and security cameras.

Keep in mind that where there is a will, there is a way, and almost no company (except for possibly Coca-Cola®) can secure the confidentiality of its trade secrets with absolute certainty. Fortunately, the law does not require bulletproof security. As long as "reasonable measures" are taken to protect the secrecy of its trade secrets, and the information is not publicly available, a company is entitled to legal protection and legal recourse against anyone who improperly accesses, uses, or discloses the company's trade secrets.

……

Sarju Naran is an attorney in Hoge Fenton's Employment Law Group, and is a valuable resource for issues concerning trade secrets, employee mobility, and unfair competition.

For more advice regarding this or any other employment or intellectual property-related question, please contact Sarju Naran at san@hogefenton.com - 408.947.2456 direct.

For more information on Hoge Fenton's trade secret practice, please click here.

This Legal Update is provided as an educational service by Hoge Fenton for clients and friends of the firm. This communiqué is an overview only, and should not be construed as legal advice or advice to take any specific action.