Every year, countless companies engage in costly litigation over the theft of their trade secrets. By the time litigation occurs, valuable trade secrets are out the door and potentially in the hands of competitors. Although injunctions can be sought to prohibit the use of these trade secrets, there is no guaranty an injunction will issue, particularly where a company has failed to take reasonable steps to protect its trade secrets. What can you do to effectively protect your trade secrets and best position yourself to obtain an injunction in the event theft occurs? The Quarles & Brady Trade Secrets & Unfair Competition Team provides you with the following tips.

**Identify Your Trade Secrets, Implement Reasonable Security Measures, and Educate Your Employees and Contractors**

**Identify Your Trade Secrets:** Conduct an audit of company information to determine what information constitutes a trade secret, keeping in mind that a trade secret is defined as:

- a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Protections available to trade secrets are typically more significant than those afforded to confidential information. For example, a claim for misappropriation of trade secrets allows for attorney fees.

**Implement Reasonable Security Measures:** Implement physical, electronic, and contract and policy-based reasonable security measures.

- The best way to avoid the misappropriation of company trade secrets is to limit access to them.
  - Examples of physical security measures include locks, gates, posted guards, ID badges, key cards, and video surveillance.
  - Electronic security measures include password protection, software that prohibits the downloading of information to portable devices, and limits on the size of emails that can be sent outside the company.
- Contractual-based security measures consist of confidentiality agreements, license agreements that specifically limit the distribution of the licensed software (and the trade secrets contained therein), and employment agreements that contain confidentiality provisions relating specifically to trade secret information, to name a few.
- Policy-based security measures include confidentiality policies, policies that require a manager to audit the issuance of all employee usernames and passwords (to ensure, for example, that an IT administrator does not set up a “dummy” account to remotely access the employer’s computer systems following his or her departure), policies that require two people to authorize the issuance of any new employee username or password or the destruction of any back-up tapes (to address the same concern), and policies that require the immediate termination of a departing employee’s access to the employer’s computer systems.
**Regularly Educate and Document:** Conduct regular employee and contractor training on the importance of maintaining trade secret information and the duty each employee has in this regard. Employees should not just focus on policing their own conduct, but should be mindful and aware of the conduct of those around them—including the conduct of co-workers, supervisors, and customers. Explain to employees the importance of maintaining the confidentiality of trade secrets, noting the adverse impact the loss of a trade secret would have on the company and its employees (most notably by way of dollars out the door). Document the training provided to employees. Have employees sign attendance sheets when attending trade secret training, and make attendance a mandatory part of the job. When employees leave your employment, conduct exit interviews and remind employees of their duty to maintain in confidence trade secret information.

When working with customers, suppliers, and other business partners, require the execution of a nondisclosure agreement prior to providing any confidential or trade secret information. When a guest visits a facility housing your trade secrets, require them to sign a nondisclosure agreement prior to admittance.

**Investigate and Prosecute**

In the event a trade secret is transmitted outside the company (either intentionally or unintentionally) you must take immediate action to cease further dissemination of the trade secret and undo the harm that has already been done.

**Identify the Source of the Breach:** Conduct computer forensic searches to determine where the breach occurred. It is advisable to retain an independent computer forensics company to conduct the analysis, particularly if you believe the matter will lead to litigation. Conduct employee interviews to determine what your employees know about the breach. Often, a thieving employee will brag about their actions to a co-worker, so co-workers can be a great source of information.

**Address the Breach:** If the breach was by way of an errant email to someone outside the company, determine why the email was sent and how to prevent future breaches. Provide employees with further training on the importance of being mindful of the persons to whom they send such information. Immediately ask the errant recipient to return or destroy the information.

If the breach was the result of intentional conduct, terminate the person who disseminated or took the information and immediately seek an injunction enjoining the use or further distribution of the information. If there is any uncertainty about the cause or the source of the breach, contact an attorney who can connect you with professionals proficient in investigating such matters. DO NOT HESITATE TO ACT. The longer the trade secret is in the public domain, the more likely it is a court will deny an injunction, and the more likely it is other companies or individuals will learn about and use it.

**Quarles Can Help**

Quarles & Brady’s Trade Secrets & Unfair Competition Team stands ready to assist you in matters involving unfair competition, including claims involving trade secret misappropriation, antitrust issues, noncompete breaches, false advertising, tortious interference with contracts and business relationships, business defamation, and breaches of the duty of loyalty. From advising you on preventive measures to litigating such matters, the attorneys on the Trade Secrets & Unfair Competition Team will use their extensive experience in this area to get the job done right. If you need assistance, contact Nicole Druckrey at 414-277-5777 or nicole.druckrey@quarles.com.