

Fundamentals of Trade Secrets

Trade secrets are most valuable in industries where the technology changes continuously and rapidly. The recent rise of industrial globalization and the increasing mobility of employees between competing companies make controlling access to and maintaining trade secrets fundamentally important. Intellectual property, which encompasses trade secrets, can average 70% of the market value of a company. A company's trade secrets lend it a competitive advantage in the marketplace and reward and promote its innovation and technological development.



What is a trade secret?

A trade secret is a confidential practice, method, process, design, or other information used by a company to compete with other businesses. It is also referred to in some jurisdictions as “confidential information.” Typically, a trade secret is characterized by some form of a competitive edge. It can be something as simple as a list of current or former customers, potential customers that the company's research shows might benefit from their services, or institutional knowledge of a customer's needs or business operations.

In order for information to be considered a trade secret, it must derive independent economic value, actual or potential, from not being generally known or readily ascertainable through proper means by the public. The company owning the trade secret must intend to keep and maintain the information as a trade secret and take reasonable measures to keep such information secret. The company cannot first treat information casually, only to later assert that it is a trade secret after some theft or misappropriation has occurred. Reasonable efforts to maintain its secrecy must be initiated before such an event. Practices that could be considered “reasonable efforts” to maintain secrecy can vary, depending on the nature of the protected information and the company's common business practices. For example, a company might limit access to sensitive information, mark documents as confidential, restrict duplication of confidential information, or educate those with access to the information about the nature of its sensitivity and appropriate means to protect it.

Introduction to Trade Secret Law

Trade secrets are not protected by law in the same manner as trademarks or patents. Secrecy, rather than full disclosure, is what defines and protects the asset. Companies seek to keep their special knowledge out of the hands of competitors through a variety of civil and commercial means, including confidentiality or nondisclosure agreements. Such agreements often require employees to sign over the rights to the ownership of their own intellectual production during the course of their employment. Similar agreements are often signed by representatives of other companies with whom the trade secret holder is dealing.



State laws govern the details of trade secret protection within the state. Most state laws define trade secrets as information that (a) is not generally known to the relevant portion of the public, (b) confers some sort of economic benefit on its holder (this benefit must derive specifically from the fact that it is not generally known, not just from the value of the information itself), and (c) is the subject of reasonable efforts to maintain its secrecy. While there is no governing federal trade secret law, many states have adopted a model set of laws. The applicable state law depends on a number of factors, including, for example, where the parties reside or where the alleged theft or misappropriation occurred. Recently, approximately 43 states adopted the Uniform Trade Secrets Act (UTSA) as the basis for their trade secret law. Many believe that a measure of uniformity among different states' laws will strengthen business' claims on their trade secrets.

The U.S. Economic Espionage Act of 1996 (18 U.S.C. §§ 1831-1839), was another major development in trade secret laws in the United States and internationally. Section 1832 of the Act made trade secret theft a federal crime and gave the Department of Justice sweeping authority to prosecute offenders in and out of the United States. A violation of Section 1832 can result in stiff criminal penalties. A person who commits an offense in violation of Section 1832 can be imprisoned up to 10 years in prison and fined up to \$500,000. A corporation or other organization can be fined up to \$5,000,000. If the trade secret theft benefits a foreign government, foreign instrumentality, or foreign agent, the penalties are even greater.



12545 White Drive
Fairfax, Virginia 22030
Tel: 202-445-2000
Fax: 888-492-1303
www.LGJlegal.com

Why do trade secrets need protecting?

Trade secret protection offers an advantage over patent protection in that it can extend indefinitely. In general, trade secret rights extend as long as the proprietary information remains secret. Once the information is made public, however, the trade secret protection is lost and cannot be recovered. The Coca Cola Company has been quite effective at protecting its soft drink formulation for much longer than the term of any patent grant. Of course, the lack of formal, documented protection means that a third party is not prevented from independently duplicating the secret information.



It is not uncommon for companies to try to discover one another's trade secrets whether through legitimate as well as improper means. Reverse engineering is permissible and is a commonly accepted practice. On the other hand, industrial espionage is illegal, and trade secrets acquired by these means are deemed misappropriated. Companies caught engaging in industrial espionage will probably be subject to legal liability unless the owner of the trade secret fails to demonstrate that it made reasonable efforts to keep the information confidential. In these cases, trade secret owners risk losing the trade secret, even if the information is obtained illegally by competitors.

Trade secrets are defined broadly in order to cover every conceivable act of trade secret misappropriation including theft, appropriation without authorization, concealment, fraud artifice, deception, copying without authorization, duplication, sketches, drawings, photographs, downloads, uploads, alterations, destruction, photocopies, transmissions, deliveries, mail, communications, or other transfers or conveyances of such trade secrets without authorization. This definition generally tracks the definition of trade secrets given in the Uniform Trade Secrets Act, but expands the definition to include the new technological ways that trade secrets are created and stored. The Act also makes it a federal criminal offense to receive, buy, or possess the trade secret information of another person knowing the same to have been stolen, appropriated, obtained or converted without the trade secret owner's authorization.



Types of information that can be considered trade secrets include:

<p>Technical Information/Research & Development Proprietary Technology Information Proprietary Information Concerning Research and Development Processes Laboratory Notebooks Experiments and Experimental Data Analytical Data Algorithms and Types of Data Calculations Drawings - All Types Diagrams - All Types Design Data and Design Manuals R & D Reports - All Types</p> <p>R & D Know-How and Negative Know-How (i.e., what does and does not work) Data Handling and Process Information Proprietary Information Concerning How Data is Handled and Processed Production Know-How & Negative Know-How</p> <p>Vendor/Supplier Information Vendor/Supplier Contact Information Terms of Supply Cost/Price Data</p>	<p>Quality Control Information Quality Control Procedures Quality Control Manuals Quality Control Records</p> <p>Sales & Marketing Information Sales Forecasts Marketing And Sales Promotion Plans Sales Call Reports Competitive Intelligence Information Proprietary Customer Lists and Contact Information Customer Needs And Buying Habits Know-How Concerning The Management Of Customer Confidence Proprietary Sales And Marketing Studies And Reports</p> <p>Internal Financial Information Internal Financial Documents Budgets Forecasts Computer Printouts Product Margins Product Costs Operating Reports Profit And Loss Statements Proprietary Administrative Information Internal Administrative Information Internal Organization Key Decision Makers Strategic Business Plans Internal Computer Software</p>
--	--