Chapter 2
Trade Secret Protection

Trade secret law provides a mechanism for protecting proprietary and sensitive business information. A trade secret, by definition, is information that has economic value and is secret. There are no formal application requirements to obtain a trade secret. Unlike patents, there are no statutory requirements that a trade secret be novel, useful, non-obvious, and there is no examination process. Trade secret protection arises once the appropriate steps are taken to create a valid trade secret. Trade secrets are not subject to a predefined term, and can be maintained for an indefinite period of time.

2.1 What Is a Trade Secret?

Unlike patent law, which has its roots firmly grounded in federal constitutional and statutory law, trade secret law is a state law doctrine that developed out of the common law doctrine of unfair competition and unfair business practices. Until passage of the Uniform Trade Secrets Act (UTSA) in 1985, trade secret law varied significantly from state to state. The UTSA is a model law that provides a uniform definition of trade secrets and misappropriation, and 45 states, the US Virgin Islands, and the District of Columbia, have adopted it.

The UTSA defines a trade secret as "information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (1) derives independent economic value, actual or potential, from no 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 (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy." This broad definition maintains the common law that nearly any type of business information can qualify as a trade secret. Thus,

R.W. O'Donnell et al., *Intellectual Property in the Food Technology Industry*,
DOI: 10.1007/978-0-387-77389-6_2,

information that is not otherwise patentable can be a trade secret. Examples of information that can be protected by trade secret include:

- computer programs
- client identities
- product pricing
- manufacturing processes
- technical information
- technical information
- prototypes
- company manuals
- financial statements
- customer lists
- vendors
- market analysis and strategies
- formulas
- product testing results (positive and negative)
- drawings
- strategic plans
- employee records and salaries
- product ingredients (foods, cosmetics, or drugs, etc.)

Because information of nearly any type of subject matter can qualify as a trade secret, the UTSA definition of a trade secret focuses on: (1) the economic value of the trade secret; (2) whether the trade secret is generally known or readily ascertainable; and (3) the efforts taken to maintain secrecy. The "economic value" requirement under the UTSA refers to whether a competitor would obtain an economic benefit if the trade secret information became readily accessible. "Economic value" can be shown by the time and effort utilized in creating the trade secret, or by showing that a third party would have to spend time and effort in creating the same trade secret.

The second requirement for a trade secret under the UTSA is that the information cannot be "generally known or readily ascertainable." This means that the information cannot be already known to the public or by competitors. Whether a trade secret is "generally known or readily ascertainable" is a factual inquiry that depends on the amount of time, effort, and money required to independently produce the trade secret, or to reverse engineer the trade secret. Information cannot be protected by a trade secret if it can be discovered by examining a commercially available product that incorporates the information. If the trade secret is hidden in a commercially available product, then the trade secret can be maintained. A trade secret that consists of the amounts and ratios of individual ingredients in a product or code

embedded in a software program is not lost just because the product becomes public availability.

Published information, such as that disclosed in a book, magazine, trade publication, website, or other media, cannot be maintained as a trade secret because it is "generally known" and readily ascertainable. This can be particularly important when deciding whether to keep information as trade secret or to pursue patent protection for that information. Anything disclosed in a patent or published patent application is generally known and readily ascertainable and cannot be protected as a trade secret.

Example: Tastewell is confident that the ratio of ingredients in its new cheese and fruit product could not be reverse engineered by a competitor analyzing its product. However, as part of a marketing strategy, Tastewell decides to pursue patent protection for the formulation of its cheese and fruit product. During examination of its patent application, the USPTO examiner asserts that Tastewell's formulation would be obvious. Tastewell is unable to convince the examiner otherwise and decides to abandon its patent application. Tastewell inquires whether its product formulation can be maintained as a trade secret now that it cannot get a patent.

If Tastewell's patent application was not published before abandonment, it may be able to maintain its production formulation as a trade secret. However, if Tastewell's patent application is published, the information is public and Tastewell cannot maintain its product formulation as a trade secret.

The final and often most important criterion for a trade secret under the UTSA is that reasonable efforts must be taken to maintain secrecy of the information. Maintaining secrecy of a trade secret is viewed under a reasonable standard which does not require absolute secrecy. A court considers several factual inquiries when considering reasonable secrecy:

- whether employees have executed confidentiality or non-disclosure agreements;
- whether the company's confidentiality policy is memorialized in writing;
- whether access to the trade secret is been limited to essential employees/contractors;
- whether employees who are privy to the trade secret are aware that it is to be maintained as a trade secret;

- whether the information is kept in a restricted area such as a locked file, within security encrypted software, in a restricted location within a physical plant, etc.;
- whether documents containing information that is trade secret are properly labeled; and
- whether the company actively screens employee publications, presentations, etc. for disclosure of trade secret information.

In addition to these factors, it is important that the owner of the trade secret takes steps to enforce secrecy of the information. Mere intent to keep information trade secret, without affirmative acts, is typically insufficient to maintain a trade secret.

2.2 Misappropriation of Trade Secrets

A trade secret owner has the right to prevent others from misappropriating the trade secret. The UTSA defines misappropriation of a trade secret as:

(i) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or
(ii) disclosure or use of a trade secret of another without express or implied consent by a person who

(A) used improper means to acquire knowledge of the trade secret; or
(B) at the time of disclosure or use knew or had reason to know that his knowledge of the trade secret was

(I) derived from or through a person who has utilized improper means to acquire it;
(II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or
(III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or

(C) before a material change of his position, knew or had reason to know that it was a trade secret ad that knowledge of it had been acquired by accident or mistake.

In summary, misappropriation is the improper acquisition, disclosure, or use of a trade secret. A trade secret can be misappropriated even if the misappropriating party is not identically duplicating the trade secret.

Trade secrets can be lost or stolen in a variety of ways. Theft, bribery, misrepresentation, or breach of a duty to maintain secrecy are common acts

that trigger a trade secret loss. Violating a confidentiality or non-disclosure agreement or obtaining the trade secret from a third party that is bound by a duty of confidentiality can give rise to an action for misappropriation. For example, a common means by which trade secrets can be lost or stolen is typically through unhappy or former employees who use or disclose the trade secret information apart from the company.

When a company discloses its trade secret to others, such as employees, manufacturers, suppliers, consultants, etc., those disclosures should be made under a written duty of confidentiality. This is typically done by requiring the party to execute a confidentiality or non-disclosure agreement, by way of employment contract, or third party consulting or supplier agreement. If a party under a duty of confidentiality with the trade secret owner breaches that duty, the trade secret owner's enforcement effort will benefit from a written agreement that clearly recognizes the trade secret status of the information.

The UTSA identifies a number of remedies for misappropriation of trade secrets including injunctions, damages, and attorney's fees. The UTSA even permits recovery of both the actual loss created by the misappropriation and any unjust enrichment resulting from the misappropriation that is not included in the "actual loss" portion of the damages. If actual loss for the misappropriation is difficult to prove, the trade secret owner may seek a "reasonable royalty" as compensation for the misappropriation. If the acts resulting in the trade secret misappropriation are willful or malicious, the UTSA grants the court discretion to award attorney's fees to the trade secret owner.

Example: Two of Tastewell's scientists, Dr. Curd and Dr. Whey, invented Tastewell's new cheese and fruit product. Subsequently, Dr. Curd resigned from Tastewell and began working for Tastewell's competitor, Bland Foods. Tastewell learned that Bland Foods began marketing a similar product almost immediately after Dr. Curd was hired. Can Tastewell take any action against Bland Foods?

Tastewell should consider an action against Bland Foods for misappropriation of trade secrets. In order to prevail, Tastewell must first establish that the cheese and fruit product was maintained as a trade secret (independent economic value, reasonable measures to maintain secrecy, and not readily ascertainable to others by proper means) and that Dr. Curd improperly disclosed it to Bland Foods. The easiest way to prove knowledge and improper disclosure is to show that

Dr. Curd had acknowledged in writing his duty to maintain Tastewell's product in secrecy (i.e., by way of a confidentiality of non-disclosure agreement) and Tastewell had written internal procedures directed to preventing disclosure.

2.3 Reverse Engineering of Trade Secrets

Under patent law, a subsequent inventor can be liable even though the invention was developed completely independently and without knowledge of the patented invention. Under trade secret law, independent discovery and use of the trade secret is not a violation. Further, competitors often try to uncover and trade off of one another's trade secrets by "reverse engineering" the trade secret; a legally acceptable practice. The comments to the UTSA state that "reverse engineering" is a proper means of discovering a trade secret and identify reverse engineering as "starting with the known product and working backward to find the method by which it was developed. The acquisition of the known product must, of course, also be by a fair and honest means, such as purchase of the item on the open market for reverse engineering to be lawful . . . ." Thus, discovery of another's trade secret requires proper acquisition of the information and ethical business practices.

Example: Once Tastewell sells its new cheese and fruit product to the public, it is permissible for any purchaser to analyze the product to determine the process by which it was produced or to determine its constituent ingredients. The purchaser has the right to use and disclose any information acquired as result of reverse engineering the product.