Bloomberg BNA

Health IT Law & Industry Report™

VOL. 8, NO. 48 NOVEMBER 28, 2016

Understanding Misappropriation of Trade Secrets

By Ryan Schultz

Employers and business owners know too well the problems that can arise when an employee leaves to take a job with a competitor.

They most often arise when an employee has strong relationships with customers with special needs and requirements, or if the employee has knowledge of sensitive business information such as the source code structure for a company's most successful product or pricing structure.

But many employers do not know what rights they have if their former employee discloses or uses the former employer's information in their new employment.

This is especially a concern in the growing healthcare IT industry. Indeed, numerous market analysts are predicting significant growth in healthcare IT over the next few years, some as high as 12 percent compound annual growth rate.

Ryan Schultz is a principal in Robins Kaplan LLP's intellectual property and technology litigation group. He is based in the firm's Minneapolis office.

In addition, non-traditional market participants are entering this market looking to gain a slice of this growing market. With this explosion of the market, the likelihood of employee movement is greatly increased.

It will be imperative for companies to protect their intellectual property with every tool in the toolbox to allow the company to remain competitive.

The Uniform Trade Secrets Act (UTSA) may provide an answer to losses caused by a former employee's disclosure of certain confidential business information to a new employer.

The UTSA is a set of laws adopted by 46 of the 50 states to provide a uniform system of rules and remedies for the wrongful acquisition, disclosure and use of a trade secret. The UTSA calls all of these ''misappropriation.''

Depending on the facts, the consequences for misappropriation of a trade secret under the UTSA can include money damages, a court-imposed royalty, and possibly an injunction preventing a competitor from doing certain business. When applicable, the UTSA offers

 ISSN 2151-2876

a powerful tool to address the wrongful acquisition, disclosure, and use of confidential information.

Defining Trade Secrets

Under the UTSA, trade secrets can be any type of information, including confidential contract terms and requirements, formulas, patterns, compilations, programs, devices, methods, techniques, or processes. To qualify as a trade secret, the information must:

1. Derive **value** from not being generally known to the public or to other people who can obtain value from its disclosure or use; and
2. Be the subject of **efforts** that are reasonable **to maintain its secrecy.**

Those claiming a trade secret must usually first prove the information's secrecy and the efforts made to maintain its confidentiality.

UTSA protection is not automatic but rather depends on showing the steps taken to keep the particular information secret. Having employees sign confidentiality agreements, regularly communicating expectations around confidentiality, and including confidentiality provisions in personnel manuals may all help show the secrecy of the information in question.

Once claimants have established secrecy, they need to show the information has value *because* it is secret, and *by being kept* a secret.

Value may exist in information, like recipes and processes, that businesses use every day as well as in information that has commercial value from not being used—as in the case when trial and error creates value by demonstrating that a certain practice does *not* work.

For growers, customer lists, supply agreements and their specifications, and proprietary production processes all serve as examples of information potentially entitled to trade secret protection.

Misappropriation of Trade Secrets Under the UTSA

The UTSA protects the wrongful acquisition, disclosure, and use of protected trade secrets. An outright theft—like breaking into a competitor's warehouse and stealing a secret formula—of course qualifies as misappropriation. But misappropriation may also occur when someone with a duty to keep a secret or limit the use of protected information discloses that information without the rightful owner's consent.

Depending on the circumstances, a former employee may have a duty to keep information secret under the terms of confidentiality agreements, as a result of company policies or because of expectations expressed in face-to-face communications.

Just going to work for a competitor is usually not enough to show misappropriation. Instead, misappropriation happens when the former employee discloses a former employer's trade secret to the new employer or when he or the new employer uses the protected information in the new employment.

Examples of situations where growers might see misappropriation occurring include instances where a former employee takes a list of customers who buy specialized produce, or have special requirements for the production, processing, and delivery of the produce, or situations where the former employee divulges confidential product processing technologies, pricing structures, production and delivery schedules, and customer requirements as part of his new employment with a competitor, particularly in markets for specialized goods.

Rights and Remedies Under the UTSA

The UTSA provides a wide range of potential relief for misappropriation of trade secrets. A business or employer bringing a claim under the UTSA may recover damages for the actual loss caused by the misappropriation and may also recover for the unjust enrichment caused by the misappropriation not taken into account in computing damages for the actual loss.

UTSA claimants can also seek an injunction stopping the threatened or actual use of trade secrets. Courts have the additional power to require affirmative actions, if necessary, to protect a trade secret such as the destruction of goods created using a trade secret, or the deletion of certain information from computers.

Alternatively, the UTSA provides for the possibility of royalty payments for the continued use of the trade secret in situations where damages or an injunction are too difficult to prove or impractical to apply. The specific remedies available will depend upon the facts of the case involved.

The Defend Trade Secrets Act

In May 2016, President Obama signed into law the Defend Trade Secret Act (DTSA). This Act provided federal cause of action for trade secret misappropriations. The DTSA defines a trade secret in the same general way as trade secrets are defined in the UTSA.

One advantage of the DTSA is the ability to seek relief in federal court rather than state court. This advantage will be important for companies that have employees in various states, as each state's implementation of the UTSA is not uniform.

For the healthcare IT industry, the types of information include processes, programs, and code, all of which are critical to the success of any healthcare IT company.

Another advantage of the DTSA is that it broadly defines what type of information could be considered a trade secret. For the healthcare IT industry, the types of information include processes, programs, and code, all of which are critical to the success of any healthcare IT company.

This expansive definition of trade secrets will allow companies to take a more proactive approach in protecting those aspects of the companies that provide an economic advantage to the company from improperly being provided or utilized by a competitor.

The DTSA provides a unique remedy beyond that provided in the UTSA. In particular, a trade secret owner may obtain an ex parte seizure order. This order

   ISSN 2151-2876

is obtained through a court proceeding where there is an immediate and extraordinary need to have the law enforcement obtain the trade secrets from the accused misappropriator.

This remedy will not be available in every situation, only those where the trade secret owner can demonstrate that the alleged misappropriator is in actual possession of the trade secrets. This requirement may make this remedy challenged to seek in the healthcare IT if the alleged misappropriator simply has knowledge of the source code structure, for example, of the company's product but does not actually have print outs of the source code.

Likewise, knowledge in a person's memory of the various pricing structures implemented by the company would not likely be the type of trade secret misappropriation wherein this remedy could be exercised.

Nevertheless, there will likely be situations that arise where having access to this remedy will be highly important.

Given the speed at which one would need to move to seek this type of relief, it is critical for companies, especially healthcare IT companies, to conduct an audit of the information the company believes is best protected by trade secret protection, adequately and properly define the information that should be protected by trade secret, assess the procedures and safeguards in place to keep the identified information secret, and provide clear instructions to employees as to what information is protected by trade secrets and what is not protected.

Lastly, the DTSA included certain protections for a whistleblower that provide information that is allegedly covered by a trade secret if that disclosure was provided to law enforcement for investigation of violation of law. Companies that seek to rely on the DTSA for trade secret protection need to update their company manuals or contracts to include the appropriate notice language provided in the DTSA.

Conclusion

Businesses make significant investments to develop and protect unique information in their business to gain competitive advantages. When part of the value of that information comes from keeping it secret—and secrecy has been maintained—the information may qualify as a trade secret.

Under the Uniform Trade Secret Act and Defend Trade Secret Act, business owners facing the disclosure of protected trade secrets to competitors by a former employee may be able to keep the information confidential and recover damages for losses caused by its wrongful disclosure or use.

Protection under the UTSA and DTSA does not happen automatically however. Determining whether or not a trade secret has been misappropriated—or whether a business may have benefited from potential trade secrets—requires careful analysis both about what was done, and how it has impacted your business.

In order to ensure the maximum protection of businesses' vital information, practices should be developed to maintain their secrecy within the company, and to implement a strategic response when circumstances arise that threaten the confidentiality and value of a business' important trade secrets. And unless disclosure or use of a trade secret is believed to have occurred, keep it a secret.