The Computer & Internet Lawyer

Volume 33 ▲ Number 9 ▲ SEPTEMBER 2016

Ronald L. Johnston, Arnold & Porter, LLP, Editor-in-Chief

Preventing Trade Secrets Theft under the New Trade Secrets Law

By Joseph F. Cleveland, Jr.

The Defend Trade Secrets Act of 2016 (DTSA), enacted earlier this year, creates a body of federal trade secret law that compliments and largely mirrors the Uniform Trade Secrets Act (UTSA), adopted in 48 states. Combined, the DTSA and UTSA now govern trade secret protection in almost every jurisdiction in the United States.

Broadly speaking, a trade secret is any information not publically known, which provides a company a competitive edge. Under both the DTSA and UTSA, trade secrets can consist of any information, including a formula, pattern, compilation, program, device, method, technique, or process. The DTSA expands this list to include all forms and types of financial, business, scientific, technical, economic, or engineering information, whether tangible or intangible, and wherever stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing.

Unlike a patent or copyright, trade secret protection can last forever. But it is an unforgiving form of protection and can be easily lost if the secret is publicly disclosed. Therefore, from the moment a trade secret is created, the owner must guard its secrecy 24 hours a day, 365 days a year. Here are some relatively simple steps that a company can take to protect its trade secrets under the DTSA and UTSA.

Step One: Identify the Trade Secret

A company should first identify the trade secrets that are crucial to the economic success of the business. Under both the DTSA and UTSA, a trade secret must be information possessing some economic value from not being generally known or readily ascertainable by others outside the company. It includes information having "actual or potential" economic value and thus includes those trade secrets that have not yet been put to

Joseph F. Cleveland, Jr. practices in the area of trade secrets litigation at Brackett & Ellis, P.C. in Fort Worth, TX. Mr. Cleveland is chair of the Trade Secrets Committee of the Intellectual Property Section of the State Bar of Texas. He routinely counsels clients on issues related to trade secrets and represents clients in trade secret cases in both state and federal courts.

Wolters Kluwer

use or that have been used or later abandoned. Similarly, trade secrets may include "negative know-how," which is information resulting from lengthy and expensive research proving that a certain formula, method, or process will not work.

Despite this expansive list of trade secrets protected under the DTSA and UTSA, a company should not simply designate every piece of technology or business information as a trade secret. When everything is a trade secret, it's just another way of saying that nothing is. A company should therefore thoughtfully consider what is worth spending the time and effort to protect.

Step Two: Maintain Secrecy

To be entitled to trade secret protection under the DTSA and UTSA, the owner must take steps that are reasonable under the circumstances to maintain the secrecy of the trade secret. Although there are a variety of actions a company can take, they should be customized to the individual business requirements of each company.

Employee Guidelines

Protecting a company's trade secrets starts with its employees. A company should provide employees with specific guidelines on the kinds of information considered to be trade secrets, inform them that this information should not be disclosed outside the company under any circumstances without written permission, explain how the company expects its trade secrets to be handled internally, and warn of serious consequences for any failure to comply. The company should periodically brief employees on these rules and require them to sign an acknowledgement that they received and understood the company's trade secret polices.

Non-Disclosure Agreements

A non-disclosure agreement (NDA) allows the company to impose contractual liability for any disclosure or misappropriation of the company's trade secrets. A typical NDA requires the employee to keep trade secrets in the strictest confidence, prohibits the employee from disclosing the information outside the company without prior written consent, and warns that the employee cannot make any use of the trade secret for the employee's benefit or the benefit of anyone else outside the company. The NDA also should make clear that the duty to maintain confidentiality remains even after termination of employment. The NDA should mirror the language from the company's trade secrets policies and inform the employee of consequences for noncompliance.

The company may consider advising employees that under the DTSA and UTSA, the company is authorized to obtain a court order to stop any actual or threatened misappropriation of its trade secrets. In addition, the company could appropriately inform its employees that the company has the right to recover damages for any misappropriation, to seek an award of exemplary damages for willful and malicious misappropriation, and to recover its reasonable attorney fees. Because neither the DTSA nor the UTSA affect criminal remedies, the company also may consider informing employees that theft of trade secrets constitutes a crime.

Under the DTSA and UTSA, the company is authorized to obtain a court order to stop any actual or threatened misappropriation of its trade secrets. In addition, the company has the right to recover damages for any misappropriation, to seek an award of exemplary damages for willful and malicious misappropriation, and to recover its reasonable attorney fees.

The DTSA requires employers to notify its employees that they are immune from civil or criminal liability if the employee: (1) discloses the company's trade secrets in confidence to a government official or to an attorney solely for the purpose of reporting or investigating a suspected violation of law; or (2) files the trade secret under seal in a court proceeding. If the company does not comply with the notice requirement, the company cannot recover exemplary damages or attorney fees against that employee to whom notice was not provided. The UTSA has no such notice requirement.

The DTSA and UTSA specifically provide that they do not preempt contractual or other civil remedies. Therefore, any employee who will be exposed to the company's trade secrets should be required to sign an NDA. Any breach of a duty to maintain secrecy under the NDA will not only result in contractual liability but also will constitute a violation of the DTSA and UTSA. In addition, a contract may provide for the recovery of attorney fees for breach of contract without a finding of willfulness, which is required under both the DTSA and UTSA.

Sub-Contractors, Vendors, and Licensees

Sub-contractors or vendors who may be exposed to the company's trade secrets should be required to

sign an NDA at the outset of the relationship. The NDA should specifically describe the trade secrets that are being disclosed, describe the purpose for the disclosure, define the scope of permitted use, and warn against any disclosure without the company's prior written consent. When temporary workers are hired, make certain they sign the company's NDA. If a formal written agreement cannot be signed, the company should at least notify the sub-contractor or vendor of the company's expectations regarding its trade secret information.

A cease and desist letter is designed to put the misappropriator of the trade secrets on notice that the company is aware of the misappropriation, that the company expects the trade secrets to be immediately returned and not disclosed, and that there will be serious consequences if the information is not returned.

Those who will obtain a license to use a company's trade secrets also should be required to sign a license agreement that contains provisions similar to the NDA. A license agreement also may prohibit reverse engineering of the trade secret.

Trade Secret Notifications

A company should notify employees and others about what information the company considers a trade secret by marking the information with a conspicuous warning. If the trade secret consists of a document, each page should be tagged or stamped. If possible, computer files containing trade secrets should be segregated and marked. Any software containing trade secrets should have a notice appearing on the logon screen. Emails or correspondence transmitting trade secret information should conspicuously state that trade secret information is enclosed. If customer or vendor information constitutes a trade secret, it should be maintained in a separate database and marked as a trade secret.

Trade Secret Controls

A company should exercise a reasonable degree of control over its trade secret information. In addition to previously mentioned efforts, access control measures could include any of the following, depending on circumstances:

- Limiting access to trade secrets to selected employees on a need-to-know basis;
- Implementing internal and external computer access controls, such as password protection, for any trade secrets that are stored electronically;
- Restricting the copying or transmitting of any trade secret information;
- Prohibiting the off-site removal of or access to trade secrets;
- Encrypting documents and emails;
- Prohibiting employees from working on sensitive company materials on their personal devices;
- Maintaining electronically stored trade secrets in read-only files;
- Tracking who accesses trade secret information and when it was returned;
- Monitoring employee computers for access to unauthorized materials;
- Installing access control measures in areas where trade secrets are stored;
- Prohibiting, limiting, or controlling employees' use of smartphones, laptops, thumb drives, external hard drives, or other storage devices in areas where trade secrets are stored;
- Shredding documents and wiping files or hard drives before disposal;
- Issuing periodic reminders to employees about the company's trade secrets policy;
- Establishing a protocol for departing employees that includes conducting formal employee exit interviews; prohibiting the deletion of any electronically stored information unless authorized in writing; requiring the documentation, return, or disposal of any trade secret information found in the employee's office or on the employee's devices; forensically examining computers to determine if the employee copied or transmitted any trade secret information, accessed any unauthorized materials, or engaged in any other questionable activities; and notifying the former employee's new employer that the employee

signed an NDA and that the company is serious about enforcing it;

- Controlling visitor access with sign-in and sign-out lists, visitor badges, and escorts;
- Instituting a formal process for having a signed NDA in place before any meetings with outsiders where trade secrets may be disclosed;
- Screening employee speeches, presentations, and marketing materials for inadvertent disclosure of trade secret information; and
- Putting someone in charge of the company's trade secret program.

Step Three: Take Action against Misappropriation

When a misappropriation of a company's trade secrets has occurred, it is important for a company to take immediate and decisive action to prevent further dissemination of the trade secret.

The DTSA and UTSA contain specific provisions for obtaining a court order for actual or threatened misappropriation of trade secrets.

Cease and Desist Letter

A cease and desist letter is designed to put the misappropriator of the trade secrets on notice that the company is aware of the misappropriation, that the company expects the trade secrets to be immediately returned and not disclosed, and that there will be serious consequences if the information is not returned. If there is an NDA, it should be enclosed and the person should be reminded of contractual obligations. If the misappropriator is a former employee, sub-contractor, or vendor, a copy of the letter should be sent to the highest-ranking official at that person's current employer. Finally, the cease and desist letter should inform the accused that misappropriation of a trade secret is a crime.

File Suit and Seek an Injunction

Both the DTSA and UTSA allow for the filing of a lawsuit against the person who: (1) acquired the trade secret by improper means; (2) disclosed or used the trade secret by improper means; or (3) disclosed or used the trade secret if the person knew or had reason to know that the trade secret was derived from or through a person who used improper means to acquire it or who was under a duty to maintain its secrecy or limit its use. The DTSA contains specific provisions for obtaining *ex parte* seizure orders in extraordinary circumstances to allow for law enforcement officials to seize the trade secret information without notice in order to prevent its dissemination. The DTSA and UTSA contain specific provisions for obtaining a court order for actual or threatened misappropriation of trade secrets. In addition, the DTSA and UTSA authorize a court to order misappropriated trade secrets to be returned to the aggrieved party.

Conclusion

Although a variety of steps can be taken to protect trade secrets, the primary objectives of a trade secret program are to: (1) identify the company's valuable trade secrets; and (2) prevent their public disclosure by making reasonable efforts under the circumstances to maintain their secrecy. Each company has its own unique needs and requirements. Thus, whatever trade secret program is adopted and implemented must be tailored to and should complement the company's existing methods of operation, employment structure, and third-party relationships.