Mum's the Word

Protecting company information under the Texas Uniform Trade Secrets Act.

BY JOSEPH F. CLEVELAND JR.

Broadly speaking, a trade secret is any nonpublicly known information that provides a company with a competitive edge. Unlike a patent or copyright, trade secret protection can last forever. But it is a very 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 2013 Texas Uniform Trade Secrets Act.[1]

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 TUTSA, a trade secret must be information that presents 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 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 TUTSA, 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 TUTSA, the owner must take steps that are reasonable under the circumstances to maintain the secrecy

of the trade secret.[2] There are a variety of actions a company can take; however, these must 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 polices.

Non-disclosure agreements. A non-disclosure agreement 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 should also 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 TUTSA, it is authorized to obtain a court order to stop any actual or threatened misappropriation of its trade secrets and has the right to recover damages for any misappropriation, to seek an award of exemplary damages for willful and malicious misappropriation, and to seek reasonable attorneys' fees for any misappropriation.[3] Because TUTSA does not affect criminal remedies,[4] the company may also consider informing employees that theft of trade secrets is a third-degree felony under Texas Penal Code section 31.05 and is punishable with up to 10 years in prison and a fine of up to $10,000.

TUTSA specifically provides that it does not affect contractual remedies.[5] 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 will also constitute a violation of TUTSA.[6] In addition, unlike TUTSA, attorneys' fees are recoverable for breach of contract without a finding of willfulness.[7]

Subcontractors, vendors, and licensees. Subcontractors 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 NDA. If a formal written agreement cannot be signed, the company should at least notify the subcontractor or vendor of expectations.

Those who will obtain a license to use a company's trade secrets should also be required to sign a license agreement that contains provisions similar to the NDA. It may also prohibit reverse engineering of the trade secret. Section 134.002(5) of TUTSA defines this as "the process of studying, analyzing, or disassembling a product or device to discover its design, structure, construction, or source code, provided that the product or device was acquired lawfully or from a person having the legal right to convey it." Section 134A.002(4) allows the discovery of a trade secret by reverse engineering unless prohibited. The language "unless prohibited" clarifies that TUTSA does not affect license agreements prohibiting reverse engineering.

Trade secret notifications. A company should notify employees and others about what information it considers a trade secret by marking the information with a conspicuous warning. If the trade secret consists of documents, 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 trade secret access to selected employees on a need-to-know basis.
- Implementing internal and external computer access controls, such as password protection.
- 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 or wiping files before disposal;
- Issuing periodic reminders to employees about the company's trade secrets policies.
- Establishing a protocol for departing employees that includes conducting formal 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.
- 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 to take immediate and decisive action to prevent further disclosure of the trade secret.

Cease-and-desist letter. A cease-and-desist letter is designed to put the misappropriator of 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, subcontractor, or vendor, a copy of the letter should be sent to the highest-ranking official at that person's current employer. The cease-and-desist letter should not threaten prosecution as it is unethical for a lawyer to present, participate in presenting, or threaten to present criminal charges solely to gain an advantage in a civil matter.[8] This rule, however, does not prohibit informing the accused that misappropriation of a trade secret is a crime.

File suit and seek an injunction. TUTSA allows an aggrieved person to file suit against the person who acquired the trade secret by improper means or 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 utilized improper means to acquire it or who was under a duty to maintain its secrecy or limit its use.[9] Section 134A.003 of TUTSA contains specific provisions for obtaining injunctive relief for actual or threatened misappropriation of trade secrets. In addition, section 134A.003(c) authorizes 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 and should complement the company's existing methods of operation, employment structure, and third-party relationships. **TBJ**

NOTES

1. Tex. Civ. Prac. & Rem. Code § 134A.002 *et seq.* (2013).
2. Tex. Civ. Prac. & Rem. Code § 134A.002(6)(B).
3. Tex. Civ. Prac. & Rem. Code § 134A.003(a), § 134A.004(a), § 134A.004(b), and § 134A.005(3), § 38.001.
4. *See* Tex. Civ. Prac. & Rem. Code § 134A.007(b)(3).
5. Tex. Civ. Prac. & Rem. Code § 134A.007(b)(1).
6. Tex. Civ. Prac. & Rem. Code § 134A.002(2).
7. Tex. Civ. Prac. & Rem. Code § 38.001 *et seq.*
8. Tex. Disciplinary R. Prof. Conduct 4.04(b) (1989).
9. Tex. Civ. Prac. & Rem. Code § 134A.002(3).

JOSEPH F. CLEVELAND JR.

practices in the areas of intellectual property and commercial litigation at Brackett & Ellis in Fort Worth. He is chair of the Trade Secrets Committee of the Intellectual Property Law Section of the State Bar of Texas and was instrumental in drafting, preparing the bill analysis, and testifying in support of the Texas Uniform Trade Secrets Act. He routinely counsels clients on issues related to trade secrets and represents clients in trade secret cases in state and federal courts.