COMMON SENSE STEPS TO PROTECT TRADE SECRETS

Joseph F. Cleveland, Jr.

Brackett & Ellis, P.C.
100 Main Street
Fort Worth, Texas 76102-3090

TexasBarCLE

ANNUAL MEETING
INTELLECTUAL PROPERTY LAW SECTION

June 19, 2015
San Antonio, Texas

CHAPTER #3

JOSEPH F. CLEVELAND, JR.
Brackett & Ellis, P.C.
100 Main Street
Fort Worth, Texas 76102-3090
Telephone: 817.339.2454
Facsimile: 817-870-2265

BIOGRAPHICAL INFORMATION

EDUCATION

B.A., Texas Christian University, *cum laude* with honors

J.D., Mississippi College School of Law with high honors

PROFESSIONAL ACTIVITIES

Shareholder, Brackett & Ellis, P.C.

Testified before the Senate Committee on State Affairs and the House Technology Committee of the 83rd Texas Legislature in support of the Texas Uniform Trade Secrets Act

Chair, Trade Secrets and Unfair Competition Committee, Intellectual Property Section, State Bar of Texas

Recognized in *The Best Lawyers in America* for Commercial and Intellectual Property Litigation

President, Federal Bar Association—Fort Worth Chapter

PUBLICATIONS

Cleveland, J. and Coffman, J.H., *Protecting Trade Secrets Made Simple: How the Recently Enacted Texas Uniform Trade Secrets Act Provides a Legislative Framework for Litigating Cases*, 76 TEX. B. J. 751 (September 2013)

Cleveland, J. and Coffman, J.H., *Should Texas Adopt the Uniform Trade Secrets Act?* NEWS FOR THE BAR, State Bar of Texas, Litigation Section (Spring 2013)

Cleveland, J. and Harrell, A., *Is Texas Becoming a Lodestar State? A Practitioner's Guide to Recovering Attorneys' Fees Under the Lodestar Method*, 75 TEX. B. J. 700 (October 2012), republished 16 JOURNAL OF CONSUMER & COMMERCIAL LAW 79, University of Houston Law Center (Spring 2013)

Cleveland, J. *Trademark Litigation*, 77 TEX. B. J. 64 (January 2014)

INTRODUCTION

Broadly speaking, a trade secret is any information that provides a company a competitive edge and is not publicly known. But to be entitled to these protections, a company must undertake some effort to maintain the secrecy of its trade secrets. In other words, it must keep its trade secrets "secret."

Unlike a patent or a copyright, trade secret protection can last forever. But it is a very unforgiving form of protection. It can be easily lost by disclosing the secret publically. Therefore, from the moment a trade secret is created, the owner must guard the secrecy of that secret 24 hours a day, 365 days a year. So how does a company maintain the secrecy of its trade secrets without simply locking the secret up and throwing away the key? Here are some reasonable and relatively simple steps that a company can take to protect its trade secrets under the new Texas Uniform Trade Secrets Act ("TUTSA"), Tex. Civ. Prac. & Rem. Code §134A.002 *et seq.* (2013).

STEP ONE: Identify the trade secret.

A company should first identify those trade secrets that are crucial to the economic success of the business. Under TUTSA, "trade secret" means:

(1) information (including a formula, pattern, compilation, program, device, methods, technique, process, financial data, or list of actual or potential customers or suppliers)
(2) that derives actual or potential independent economic value (actual or potential) from not being generally known or readily ascertainable by proper means
(3) by other persons who can obtain economic value from its disclosure or use. Tex. Civ. Prac. & Rem. Code §134A.002(6)(A).

Therefore, under TUTSA, a trade secret must be information having some economic value from not being generally know 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 so-called "negative know-how"—that 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. Therefore, a company should carefully inventory and identify those secrets that are worth spending the time and effort to protect.

STEP TWO: Take reasonable measures to maintain the secrecy of the trade secret.

To be entitled to trade secret protection under TUTSA, the owner must take reasonable steps to maintain the secrecy of the trade secret. The comments to the Uniform Trade Secrets Act explain that "courts do not require extreme or unduly expensive procedures be taken to protect trade secrets . . . ." Uniform Trade Secret Act § 1 cmt. Instead, TUTSA simply requires that the business undertake efforts to maintain the secrecy of the trade secret that are reasonable under the circumstances. Tex. Civ. Prac. & Rem. Code §134A.002(6)(B)

There are a variety of reasonable steps a company can take to secure its trade secrets. Any trade secret program, however, 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 its employees specific guidelines as to the types or categories of information the company considers its trade secrets, inform its employees 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 inside the company, and warn of serious consequences for any failure to comply. The company should periodically brief its employees about these guidelines and require the employees to sign an acknowledgement that they received and understood the company's trade secret polices.

Non-Disclosure Agreements. A Non-Disclosure Agreement (or 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 the company's trade secrets in the strictest confidence, prohibits the employee from disclosing the information outside the company without the company's 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 the confidentiality of the company's trade secrets remains even after the termination of employment. The NDA should track the language from the company's trade secrets

policy and inform the employee that if the employee fails to comply with the NDA, there will be severe consequences.

- The company may consider advising employees in the NDA that under TUTSA:
- The company is authorized to obtain a court order to stop any actual or threatened misappropriation of its trade secrets under Tex. Civ. Prac. & Rem. Code §134A.003(a).
- The company has the right to recover damages for any misappropriation of its trade secrets under Tex. Civ. Prac. & Rem. Code §134A.004(a).
- The company has the right to seek an award of exemplary damages if willful and malicious misappropriation is proven by clear and convincing evidence under Tex. Civ. Prac. & Rem. Code §134A.004(b).
- The court may also award reasonable attorney's fees for any misappropriation under Tex. Civ. Prac. & Rem. Code §§ 134A.005(3) and 38.001, *et seq*.
- Because TUTSA does not affect criminal remedies, *see* Tex. Civ. Prac. & Rem. Code §134A.007(b)(3), the company may also consider informing employees that theft of trade secrets is a third degree felony under Texas Penal Code §31.05 and is punishable up to 10 years in prison and a fine of up to $10,000.

TUTSA specifically provides that the Act does not affect contractual remedies. Tex. Civ. Prac. & Rem. Code §134A.007(b)(1). Therefore, any employee who will be exposed to the company's trade secrets should be required to sign a NDA contractually obligating that employee to maintain the secrecy of the company's trade secrets during and after employment. 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. Tex. Civ. Prac. & Rem. Code § 134A.002(2). In addition, unlike TUTSA, attorney's fees are recoverable for breach of contract without a finding of willfulness. Tex. Civ. Prac. & Rem. Code §38.001 *et. seq.*

Sub-Contractor and Vendor Agreements. Sub-Contractors or vendors who may be exposed to the company's trade secrets should be required to sign a 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 the permitted use of the trade secret, and warn against any disclosure of the trade secret without the company's prior written consent. If a formal written agreement cannot be signed, the company should at least notify the sub-contractor or vendor of the company's expectation that the company's trade secrets remain secret.

License Agreements. Licensees who will obtain a license to use a company's trade secrets should be required to sign a license agreement. The license agreement should describe what trade secrets are being licensed, define the scope of the permitted use of the trade secret, and warn against any disclosure of the trade secret without the company's prior written consent.

The license agreement may also prohibit reverse engineering of the trade secret. Section 134.002(5) of TUTSA defines "reverse engineering" 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 the company considers a trade secret by marking the information with a conspicuous warning. If the trade secret information consists of documents, each page should be marked, tagged or stamped with an appropriate warning to indicate that the company considers the information a trade secret. If possible, computer files containing trade secrets should be segregated and marked as trade secret. Any software containing trade secrets should have a notice appearing on the log-on screen indicating the software is trade secret and should not be used without written authorization. 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 on a separate database and marked as trade secret.

Trade Secret Controls. A company should exercise a reasonable degree of control over its trade secret information. Depending on the circumstances, methods of control could include:

- 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 electronically stored.
- Restricting the copying or transmitting of any trade secret information.
- Prohibiting the removal of or access to trade secrets off-site or remotely.
- Prohibiting or limiting employees from working on company materials on their home computer or 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 (such as physical or virtual locks or other forms of restricted access) in areas where trade secrets are stored.
- Prohibiting, limiting or controlling employee's use of smart phones, laptops, thumb drives, external hard drives or other storage devices in areas where trade secrets are stored
- Shredding documents or wiping files that contain trade secret information before disposal.
- Issuing periodic reminders to employees about the company's trade secrets policy
- Conducting formal employee exit interviews.
- Prohibiting the departing employee from deleting any electronically-stored information on company computers (including personal information) unless authorized in writing.
- Requiring the departing employee to document the return or disposal of any trade secret information found in the employee's office or on the employee's work computers, home computers, smart phones, or other storage devices.
- Forensically examining departing employees' work computer to determine if, within the last several months, the employee copied or transmitted any trade secret information, accessed any unauthorized materials, or engaged in any other questionable activities regarding the company's trade secrets.
- Notifying the former employee's new employer that the employee has signed an NDA and that the company is serious about enforcing it.
- Control visitor access with sign-in and 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.

STEP THREE: Take action against anyone suspected of misappropriation.

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

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 that its trade secrets have been misappropriated, that the company expects the trade secrets to be immediately returned and not disclosed, and that if the information is not returned, there will be serious consequences. If there is a NDA, it should be enclosed and the person should be reminded of the contractual obligations in the NDA. 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. The cease and desist letter should not threaten criminal prosecution. 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. Texas Rules of Professional Conduct Rule 4.04(b).

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. Section 134A.002(3). 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 a party to return misappropriated trade secrets to the aggrieved party.

CONCLUSION.

Although there are a wide variety of steps that can be taken to protect trade secrets, the primary objectives of a trade secret program is 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. Therefore, whatever trade secret program is adopted and implemented must be tailored and compliment the company's existing methods of operation, employment structure, and third party relationships