

# **2017 Texas Trade Secrets Update**

**Joseph F. Cleveland, Jr.**  
**J. Heath Coffman**  
**Jared D. Wilkinson**

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

Institute for Law and Technology

**55<sup>th</sup> Annual**

**CONFERENCE ON INTELLECTUAL PROPERTY LAW**

November 13-14, 2017

Plano

## I. OVERVIEW OF THE TEXAS UNIFORM TRADE SECRETS ACT

### A. Defining Trade Secrets

The first step in protecting a trade-secret is to identify the type of information that qualifies as a trade secret. Under TUTSA, information must meet two requirements in order for it to qualify as a trade secret: (1) it must be the subject of efforts that are reasonable under the circumstances to maintain its secrecy; and (2) it must derive independent economic value, actual or potential, from not 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. TEX. CIV. PRAC. & REM. CODE ANN. § 134A.002(6).

#### 1. Subject of Efforts That Are Reasonable Under the Circumstances to Maintain Its Secrecy

The first prong of TUTSA's trade secret definition is the maintenance requirement. It is not enough for the information to be secret; the owner must also maintain that secrecy through efforts that are reasonable under the circumstances. *Id.* § 134A.006. Reasonableness will vary based on the size of the business and the importance of the trade secret. What is reasonable for a three-person startup will rarely be reasonable for a multi-national publicly-traded corporation. Evidence of reasonable efforts to protect a trade secret can include:

- Labeling the information as confidential;
- Requiring the employees, independent contractors, and customers to sign of a non-disclosure agreement before viewing the information;
- Implementing employee guidelines that require certain information be kept confidential;
- Maintaining access controls over the information such as passwords, encryption or printing and copying restrictions;
- Storing the information in a separate protected server or file cabinet;
- Tracking who accesses the information; and
- Conducting exit interviews with departing employees to ensure all copies of the information have been returned.

*See Cleveland, J., Mum's the Word: Protecting Company Information Under the Texas Uniform Trade Secrets Act, 79 TEX. B.J. 86 (February 2016).*

#### 2. Information Must Derive Independent Economic Value From Not Being Generally Known or Readily Ascertainable

The second prong of TUTSA's trade-secret definition is the secrecy requirement. There must be some value to the trade secret because of the fact that it is unknown and not readily ascertainable to others. Perhaps the best known example of a trade secret with this economic value is Coca-Cola's

secret recipe. The recipe itself has value because Coca-Cola's competitors do not know its contents and therefore cannot offer the same product.

Typically, the economic value of a trade secret is established through the testimony of an expert or corporate representative. Furthermore, this value is not limited to intrinsic economic value—e.g., resources spent in development of trade secret or profits derived from the sale of the trade secret. TUTSA also protects “negative know-how”—i.e., “information that has commercial value from a negative viewpoint, for example the results of lengthy and expensive research which proves that a certain process will not work could be of great value to a competitor.” UTSA § 1 cmt.

Of course, if the information is known or can be readily ascertained by proper means, the information will not qualify as a trade secret. Information that can be readily ascertained by proper means is information discovered by (1) independent development, (2) reverse engineering unless prohibited (such as by a license agreement), or (3) any other means that are not improper. TEX. CIV. PRAC. & REM. CODE ANN. § 134A.002(4). Improper means of discovery includes “theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, to limit use, or to prohibit discovery of a trade secret, or espionage through electronic or other means.” *Id.* § 134A.002(2).

## **B. Claim for Misappropriation of Trade Secrets**

The elements of a TUTSA misappropriation claim are: (1) plaintiff was an owner of the trade secret and (2) the trade secret was misappropriated. TEX. CIV. PRAC. & REM. CODE ANN. § 134A.002.

### **1. Plaintiff Was the Owner of the Trade Secret**

Previously, TUTSA did not provide any guidance as to who was a proper plaintiff to sue for misappropriation of trade secrets. The Texas legislature has since amended TUTSA to define “owner”:

“Owner” means, with respect to a trade secret, the person or entity in whom or in which rightful, legal, or equitable title to, or the right to enforce rights in, the trade secret is reposed.

### **2. Defendant Misappropriated the Trade Secret**

TUTSA's definition of misappropriation is complicated, and it is frequently misinterpreted by both the courts and litigants. *See His Co., Inc. v. Stover*, No. 4:15-CV-00842, 2016 WL 4376611, at \*4 (S.D. Tex. Aug. 15, 2016), *vacated as moot*, No. 4:15-CV-00842, 2016 WL 6134939 (S.D. Tex. Sept. 8, 2016) (collecting cases). Under TUTSA, there are six alternative paths to liability:

#### **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 [§ 134A.002 (3)(A)]**

Under path one, the mere acquisition of another's trade secret is a basis for liability so long as that person has reason to know that the trade secret was acquired by improper means. For example, if an employer hired a new employee who possessed trade-secret information from his former employer, the new employer could be liable for misappropriation if the new employer had reason to know that the information provided by the new employee was acquired by improper means. The employee could also be liable under this path. However, if that employee obtained the

information through proper means—such as disclosure pursuant to the former employer’s confidentiality or non-disclosure agreement—neither the new employer nor the new employee would be liable under this path. *Educ. Mgmt. Servs., LLC v. Tracey*, 102 F. Supp. 3d 906, 913–15 (W.D. Tex. 2015) (analyzing liability where plaintiff alleged that defendant acquired its trade secrets through improper means).

**ii. Disclosure or use of a trade secret of another without express or implied consent by a person who used improper means to acquire knowledge of the trade secret [§ 134A.002 (3)(B)(i)]**

Under path two, any person who discloses or uses another’s trade secret and who acquired that trade secret through improper means could be liable for misappropriation. For example, an employee who steals a password to obtain access to his employer’s trade secret could be liable for misappropriation if that employee discloses or uses that trade secret. However, an employee who merely misuses or discloses trade secrets that were properly disclosed to him—such as through a confidentiality or non-disclosure agreement—would not be liable under this path. *Id.*

**iii. Disclosure or use of a trade secret of another without express or implied consent by a person who, at the time of disclosure or use, knew or had reason to know that the person’s knowledge of the trade secret was derived from or through a person who used improper means to acquire it [§ 134A.002 (3)(B)(ii)(a)]**

Path three is similar to path two, but it imposes liability on defendants who are further removed from the improper means of acquisition. Under path three, the employer who discloses or uses the new employee’s information is liable if the employer knew or had reason to know that the new employee utilized improper means to obtain the trade secret.

**iv. Disclosure or use of a trade secret of another without express or implied consent by a person who, at the time of disclosure or use, knew or had reason to know that the person's knowledge of the trade secret was acquired under circumstances giving rise to a duty to maintain the secrecy of or limit the use of the trade secret [§ 134A.002 (3)(B)(ii)(b)]**

Path four relates to persons who misuse or improperly disclose trade secrets that were acquired under proper means. The plaintiff must show that the defendant permissibly acquired the information within a relationship of confidence and later disclosed or used the information in violation of that confidence. *Lifesize, Inc. v. Chimene*, 1:16-CV-1109, 2017 WL 1532609, at \*9 (W.D. Tex. Apr. 26, 2017). For example, if an employee received trade secret information pursuant to a non-disclosure agreement and then disclosed that information to a competitor in violation of the non-disclosure agreement, the employee would be liable under path four. *His Co.*, 2016 WL 4376611, at \*6–7.

- v. **Disclosure or use of a trade secret of another without express or implied consent by a person who, at the time of disclosure or use, knew or had reason to know that the person’s knowledge of the trade secret was derived from or through a person who owed a duty to the person seeking relief to maintain the secrecy or limit the use of the trade secret [§ 134A.002 (3)(B)(ii)(c)]**

Path five imposes liability on a person who discloses or uses trade secret information obtained from the person in path four—i.e., it imposes liability on the employer who discloses or uses the trade secrets obtained through the new employee who owed a duty to maintain the secrecy or limit the use of his or her former employer’s trade secret.

- vi. **Disclosure or use of a trade secret of another without express or implied consent by a person who, before a material change of the position of the person, knew or had reason to know that the trade secret was a trade secret and that knowledge of the trade secret had been acquired by accident or mistake [§ 134A.002 (3)(B)(iii)]**

Path six imposes liability on the person who obtained the trade secret through accident or mistake. For example, if the new employer did not know that its new employee had obtained the trade secret through improper means or pursuant to a duty to maintain its confidentiality or limit its use, the new employer may still be liable if it later had reason to discover the trade secret and had not materially changed its position. There is currently no Texas case law as to what constitutes a material change in position. A material change in position might be a company’s investment in the production of a product that unknowingly contained another’s trade secret. In that situation, even if the company was later put on notice of the trade secret, the company may not be liable for future production if it can prove that it materially changed its position.

### C. Injunctive Relief

TUTSA provides that “[a]ctual or threatened misappropriation may be enjoined.” TEX. CIV. PRAC. & REM. CODE ANN. § 134A.003(a). A handful of courts have interpreted the phrase “threatened misappropriation” to allow injunctive relief not just when a trade secret is disclosed but also when a trade secret will be inevitably disclosed. *See, e.g., Bayer Corp. v. Roche Molecular Sys.*, 72 F. Supp. 2d 1111, 1117–20 (N.D. Cal. 1999) (collecting cases). Under the “inevitable disclosure” doctrine, a court can enjoin a former employee from using or disclosing the former employer’s trade secrets if the former employee performed duties that would necessarily cause that employee to use or disclose the former employer’s trade secrets. *Cardinal Health Staffing Network v. Bowen*, 106 S.W.3d 230, 242 n.12 (Tex. App.—Houston [1st Dist.] 2003, no pet.). One Texas court of appeals has noted that “no Texas case [has] expressly adopt[ed] the inevitable disclosure doctrine, and it is unclear to what extent Texas courts might adopt it . . . .” *Id.* at 242. However, other Texas courts of appeals have adopted or applied modified tests with similar attributes to the inevitable disclosure doctrine, holding that an employee could be enjoined from using a former employer’s confidential information “when it is *probable* that the former employee will use the confidential information for his benefit (or his new employer’s benefit) or to the detriment of his former employer.” *See, e.g., Conley v. DSC Commc’ns Corp.*, Cause No. 05-98-01051, 1999 WL 89955, at \*4 (Tex. App.—Dallas Feb. 24, 1999, no pet.) (emphasis in original); *see also T-N-T Motorsports v. Hennessey Motorsports*, 965 S.W.2d 18, (Tex. App.—Houston [1st Dist.] 1998, pet. dismissed); *Rugen v. Interactive Bus. Sys., Inc.*, 864 S.W.2d 548, 552 (Tex. App.—Dallas 1993, no writ); *Williams v. Compressor Eng’g Corp.*, 704 S.W.2d 469, 470–72 (Tex. App.—Houston [14th Dist.] 1986, writ refused n.r.e.). Neither TUTSA nor its case law have conclusively determined what “threatened”

misappropriation means under the statute. *See St. Jude Med. S.C., Inc. v. Janssen–Counotte*, No. A-14-CA-00877-SS, 2015 WL 11438611, at \*3 (W.D. Tex. Oct. 30, 2015) (applying the common law test from *Conley* and *Cardinal Health Staffing*); *see also* Harrell, A., *Is Anything Inevitable?*, 76 TEX. B.J. 757 (Sept. 2013).

Regardless of the standard used, the injunctive relief provided may either be prohibitive—such as barring the use of trade secret or even barring certain employment—or may be affirmative—such as returning the trade secret or destroying copies of the trade secret. TEX. CIV. PRAC. & REM. CODE ANN. § 134A.003(c); UTSA § 2 cmt. The court in exceptional circumstances can even order an injunction that conditions future use of the trade secret upon payment of a reasonable royalty for no longer than the period of time for which use could have been prohibited. TEX. CIV. PRAC. & REM. CODE ANN. § 134A.003(b). TUTSA defines exceptional circumstances as including “a material and prejudicial change of position before acquiring knowledge or reason to know of misappropriation that renders a prohibitive injunction inequitable.” *Id.* For example, if the defendant under path six already produced the product incorporating the trade secret before learning of the misappropriation, it might be more appropriate for the court to order the defendant to pay a reasonable royalty rather than enjoin the sale of the product.

An injunction granted under TUTSA will last only until the trade secret has ceased to exist or “for an additional reasonable period of time in order to eliminate commercial advantage that otherwise would be derived from the misappropriation.” TEX. CIV. PRAC. & REM. CODE ANN. § 134A.003(a). For example, if good faith competitors have caught up with the misappropriator by the time the case is decided, the injunction should be dissolved. UTSA § 2 cmt.

#### **D. TUTSA Damages**

Damages under TUTSA include both (1) the actual loss caused by misappropriation and (2) the unjust enrichment caused by misappropriation that is not taken into account in computing actual loss. TEX. CIV. PRAC. & REM. CODE ANN. § 134A.004(a). Actual loss would include lost profits, and unjust enrichment would include the defendant’s profits. *Carbo Ceramics, Inc. v. Keefe*, 166 Fed. App’x 714, 722 (5th Cir. 2006). Alternatively, the plaintiff can seek a reasonable royalty for a misappropriator’s unauthorized disclosure or use of a trade secret. TEX. CIV. PRAC. & REM. CODE ANN. § 134A.004(a). These damages are “[i]n addition to or in lieu of injunctive relief,” making clear that an injunction under TUTSA does not foreclose the right to recover damages as well. *Id.*

Exemplary damages are available if “willful and malicious misappropriation is proven by clear and convincing evidence.” *Id.* § 134A.004(b). Previously, TUTSA failed to define “willful,” “malicious,” or “clear and convincing,” but the Texas Legislature recently amended the statute to define all three. *See infra* Part II.E. Exemplary damages under TUTSA are limited to an amount not exceeding twice any award of actual damages. TEX. CIV. PRAC. & REM. CODE ANN. § 134A.004(b).

#### **E. Attorneys’ Fees Under TUTSA**

A prevailing plaintiff may recover attorneys’ fees under TUTSA only if it proves that (1) a motion to terminate an injunction was made in bad faith or (2) willful and malicious misappropriation exists. *Id.* § 134A.005. In contrast, a prevailing defendant may recover attorneys’ fees under TUTSA only if it proves that (1) a claim of misappropriation was made in bad faith or (2) motion to terminate an injunction was resisted in bad faith. *Id.* TUTSA does not provide a definition of “prevailing.”

## F. Miscellaneous TUTSA Provisions

### 1. Preservation of Secrecy

Under TUTSA, the trial court must “preserve the secrecy of an alleged trade secret by reasonable means.” *Id.* § 134A.006. TUTSA establishes a “presumption in favor of granting protective orders to preserve the secrecy of trade secrets.” *Id.* TUTSA further provides that protective orders may include: (1) provisions limiting access to confidential information to only the attorneys and their experts, (2) holding in camera hearings, (3) sealing the records of the action, and (4) ordering any person involved in the litigation not to disclose an alleged trade secret without prior court approval. *Id.* The intent of this provision was to eliminate the hurdles to protecting trade secret information to litigants, including eliminating Texas Rule of Civil Procedure’s 76(a)’s burdensome and outdated procedure to seal court records. *See also id.* § 134A.007(c) (“To the extent that this chapter conflicts with the Texas Rules of Civil Procedure, this chapter controls.”)

In 2016, the Texas Supreme Court case of *In re M-I L.L.C.*, 505 S.W.3d 569 (Tex. 2016) addressed whether due process required a defendant’s representative to be present at a hearing or trial where evidence of Plaintiff’s trade secrets would be introduced. *Id.* at 575–76. In 2017, the Texas Legislature adopted the court’s analysis and added certain provisions to TUTSA. Under both standards, the trial court is required to balance the due process presumption in favor of the defendant’s participation at trial against the degree of competitive harm the plaintiff would have suffered from the dissemination of the trade secret. *Id.* To make that determination, the trial court must consider the following factors:

- **The relative value of the plaintiff’s trade secrets.** The higher the value of the trade secret, the more competitive harm would come from the trade secret’s dissemination.
- **Whether defendant’s representative acts as a competitive decision-maker for defendant.** According to the Court, if the representative acted as competitive decision maker, then the disclosure of plaintiff’s trade secrets to him “would necessarily entail greater competitive harm because, even when acting in good faith, [the representative] could not resist acting on what he may learn.” (The Court’s language here seems to be an implicit acknowledgement of the inevitable disclosure doctrine.)
- **The degree to which the defendant’s claims would be impaired by the representative’s exclusion.** To make this determination, the trial court may consider the representative’s role in the organization and whether, by virtue of that role, the representative possessed specialized expertise that would not be available to defendant’s outside experts.
- **The stage of the proceedings.**
- **Whether the owner is alleging that the other party is already in possession of the alleged trade secret.** This factor was not addressed in *M-I L.L.C.* This factor was added by the Texas Legislature in 2017. *See infra* Part II.G.

## **2. Statute of Limitations**

A trade secret claim is governed by the three-year statute of limitations period found in Texas Civil Practice and Remedies Code Section 16.010.

## **3. Effect on Other Law**

TUTSA displaces conflicting tort, restitutionary, and other law of this state providing civil remedies for misappropriation of a trade secret. TEX. CIV. PRAC. & REM. CODE ANN. § 134A.007(a). TUTSA, however, does not affect (1) contractual remedies, whether or not based upon misappropriation of a trade secret; (2) other civil remedies that are not based upon misappropriation of a trade secret; or (3) criminal remedies, whether or not based upon misappropriation of a trade secret. *Id.* § 134A.007(b).

TUTSA eliminated civil liability under Texas Theft Liability Act. *His Co., Inc. v. Stover*, No. 4:15-CV-00842, 2016 WL 4376611, at \*3 (S.D. Tex. Aug. 15, 2016), *vacated as moot*, No. 4:15-CV-00842, 2016 WL 6134939 (S.D. Tex. Sept. 8, 2016). However, at least one case suggests in dicta that common law misappropriation may not have been eliminated by TUTSA. *Raybourne & Dean Consulting, Ltd. v. Metrica, Inc. & Metrica Relocations Plus, Inc.*, No. SA-14-CA-918-OLG, 2015 WL 12866214, at \*10 (W.D. Tex. Apr. 10, 2015). The language in this case is in direct conflict with TUTSA.

## **4. Uniformity of Application and Construction**

TUTSA is to “be applied and construed to effectuate its general purpose to make uniform the law with respect to the subject of this chapter among states enacting it.” TEX. CIV. PRAC. & REM. CODE ANN. § 134A.008. Therefore, Texas courts may look to other jurisdictions’ cases interpreting UTSA for guidance on TUTSA’s provisions.

## **II. TEXAS LEGISLATURE ENACTS NEW AMENDMENTS TO THE TEXAS UNIFORM TRADE SECRET ACT**

Since the passage of TUTSA in 2013, two significant events occurred. First, in May 2016, Congress passed the Defend Trade Secrets Act (DTSA), an amendment to the Economic Espionage Act of 1996, 18 U.S.C. §§ 1831–36. DTSA is a federal law that creates a civil cause of action for misappropriation of trade secrets. Like TUTSA, DTSA is largely based on the Uniform Trade Secrets Act; however, there were some minor differences that could result in non-uniform application of trade secret law in Texas. Second, the Texas Supreme Court decided *In re M-I, L.L.C.*, 505 S.W.3d 569 (Tex. 2016), which held that even in trade-secret misappropriation cases, there is a presumption that a party is allowed to participate and assist in the defense and that this presumption can only be overcome if the trial court balances certain factors.

In the 2017 Legislative Session, House Bill 1995 was introduced to address these new developments. The bill passed unanimously in the House and Senate and was one of the earliest bills signed into law by Governor Greg Abbott. House Bill 1995 amended TUTSA to make some of its provisions coextensive with DTSA to eliminate confusion and to avoid possible forum shopping between state and federal courts. In particular, the amendment makes several changes to the definitions found in TUTSA. For example, the amendment modifies the definition of “trade



secret” and includes additional illustrative examples. It also adds new definitions for “clear and convincing” evidence and for “willful and malicious” misappropriation. In addition, the amendment preserves the common law rule that an employee cannot be enjoined from using general knowledge, skill, and experience that the employee acquires during employment. Finally, the amendment codifies the Texas Supreme Court’s holding in *In re M-I, L.L.C.* regarding the circumstances in which a court may limit a party’s access to the other party’s trade secrets during trial.

TUTSA, as amended, is now the most modern and comprehensive law on trade secrets in the nation.

### **A. Trade Secret**

The amendment modifies the definition of “trade secrets” to align the definition with the definition found in DTSA:

“Trade secret” means all forms and types of information, including business, scientific, technical, economic, or engineering information, and any [a] formula, design, prototype, pattern, plan, compilation, program device, program, code, device, method, technique, process, procedure, financial data, or list of actual or potential customers or suppliers, whether tangible or intangible and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if.

(A) the owner of the trade secret has taken reasonable measures under the circumstances to keep the information secret; and

(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the [its] disclosure or use of the information.

TUTSA’s revised trade-secret definition, however, has one important difference from the definition found in DTSA. DTSA limits a trade secret to “financial, business, scientific, technical, economic, or engineering information.” 18 U.S.C. § 1839(3). In contrast, TUTSA’s revised definition provides that a trade secret can be any form or type of information and lists “business, scientific, technical, economic, or engineering information” as illustrative examples. Thus, TUTSA’s definition is broader. In addition, TUTSA specifically includes a “list of actual or potential customers or suppliers” as an example of trade secret information.

The amendment also changes the hierarchical order of sections (A) and (B) to rank the taking of “reasonable measures under the circumstances to keep the information secret” as the first requirement for meeting the definition of a trade secret. This non-substantive change mirrors DTSA and emphasizes the fact that if an owner fails to keep the information a secret, the trade secret is lost.

### **B. Misappropriation**

The amendment also makes minor, non-substantive changes to the definition of “misappropriation”:

“Misappropriation” means:

- (A) 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
- (B) disclosure or use of a trade secret of another without express or implied consent by a person who:
  - (i) used improper means to acquire knowledge of the trade secret;
  - (ii) at the time of disclosure or use, knew or had reason to know that the person's knowledge of the trade secret was:
    - (a) derived from or through a person who used ~~had utilized~~ improper means to acquire the trade secret [it];
    - (b) acquired under circumstances giving rise to a duty to maintain the [its] secrecy of or limit the [its] use of the trade secret; or
    - (c) derived from or through a person who owed a duty to the person seeking relief to maintain the [its] secrecy of or limit the [its] use of the trade secret; or
  - (iii) before a material change of the position of the person [~~person's position~~], knew or had reason to know that the trade secret [it] was a trade secret and that knowledge of the trade secret [it] had been acquired by accident or mistake.

### **C. Ownership**

TUTSA never expressly required ownership of a trade secret in order for a person to have standing to bring a claim. *LBDS Holding Co., LLC v. ISOL Tech. Inc.*, No. 6:11-CV-428, 2014 WL 892126, at \*1 (E.D. Tex., Mar. 2, 2014). At least one court, however, concluded that ownership of a trade secret was an element of a trade secret claim. *St. Jude Med. S.C., Inc. v. Janssen-Counotte*, No. A-14-CA-877-SS, 2014 WL 7237411, at \*14 (W.D. Tex. Dec. 17, 2014). The amendment clarifies that certain non-owners, like licensees, may have the right to file a claim under TUTSA. Relying on a modified definition of “owner” found in DTSA, the amendment provides that:

“Owner” means, with respect to a trade secret, the person or entity in whom or in which rightful, legal, or equitable title to, or the right to enforce rights in, the trade secret is reposed.

### **D. Clear and Convincing Evidence**

Under TUTSA, “clear and convincing” evidence of willful and malicious misappropriation is required to support an award of exemplary damages. TEX. CIV. PRAC. & REM. CODE § 134A.004(b). TUTSA, however, never defined the phrase “clear and convincing.” The amendment now defines that phrase by using the definition found in the Texas Civil Practice and Remedies Code section 41.001(2), which provides that:

“Clear and convincing” means the measure or degree of proof that will produce in the mind of the trier of fact a firm belief or conviction as to the truth of the allegations sought to be established.

### **E. Willful and Malicious**

Under TUTSA, a trade-secret owner must establish “willful and malicious” misappropriation to support an award of exemplary damages and attorneys’ fees. TEX. CIV. PRAC. & REM. CODE §§ 134A.004(b), 134A.005(a). The amendment adds a new definition for “willful and malicious.” The language is derived from the definition articulated by the Seventh Circuit in *Learning Curve Toys, Inc. v. PlayWood Toys, Inc.*, 342 F.3d 714, 730 (7th Cir. 2003) (applying the Illinois Uniform Trade Secret Act). The amendment provides that:

“Willful and malicious misappropriation” means intentional misappropriation resulting from the conscious disregard of the rights of the owner of the trade secret.

### **F. General Knowledge, Skill, and Experience**

The amendment also preserves the common law rule that an employee cannot be enjoined “from using the general knowledge, skill, and experience acquired during employment,” *Sharma v. Vinmar Int’l, Ltd.*, 231 S.W.3d 405, 424 (Tex. App.—Houston [14th Dist.] 2007, pet. dism’d). The amendment provides that:

Actual or threatened misappropriation may be enjoined if the order does not prohibit a person from using general knowledge, skill, and experience that person acquired during employment.

This language was added as a legislative check to ensure that a trade-secret owner’s efforts to protect “intangible” trade secrets as found in the revised definition of “trade secret” did not override this important common law rule.

### **G. Limiting a Party’s Access to Trade Secrets**

Finally, the amendment codifies the Texas Supreme Court’s holding in *In re M-I L.L.C.*, 505 S.W.3d 569 (Tex. 2016) and provides that:

(b) In an action under this chapter, a presumption exists that a party is allowed to participate and assist counsel in the presentation of the party's case. At any stage of the action, the court may exclude a party and the party's representative or limit a party's access to the alleged trade secret of another party if other countervailing interests overcome the presumption. In making this determination, the court must conduct a balancing test that considers:

- (1) the value of an owner's alleged trade secret;
- (2) the degree of competitive harm an owner would suffer from the dissemination of the owner's alleged trade secret to the other party;
- (3) whether the owner is alleging that the other party is already in possession of the alleged trade secret;

- (4) whether a party’s representative acts as a competitive decision maker;
- (5) the degree to which a party’s defense would be impaired by limiting that party’s access to the alleged trade secret;
- (6) whether a party or a party’s representative possesses specialized expertise that would not be available to a party’s outside expert; and
- (7) the stage of the action.

The amendment contemplates that a court must use this seven-factor balancing test to exclude a party or a party’s representative at any stage of the proceedings, including discovery, pre-trial, or trial. The amendment adds an additional factor not found in the Supreme Court’s decision: “whether the owner is alleging that the other party is already in possession of the alleged trade secret.” This factor was added because if the trade-secret owner alleges that the misappropriator already possesses the owner’s trade secret, there is little harm if that party participates in the proceeding. Conversely, potential harm could result if a party participates in the proceeding but has not yet accessed the trade secret information—e.g., where an employer hires a new employee who is in possession of another’s trade secret but the employee has not yet disclosed that secret to his new employer.

#### **H. Sealing Court Records**

An earlier version of House Bill 1995 included an amendment to section 134A.006 of TUTSA, that provided that the court’s discretionary power to seal court records exists “[n]otwithstanding any other law, including Rule 76a, Texas Rules of Civil Procedure . . .” Section 134A.006, however, already granted trial courts the discretionary power to seal court records in order to preserve the secrecy of any alleged trade secrets. The court’s existing power to seal court records under TUTSA, combined with the fact that TUTSA explicitly controls over conflicting Texas Rules of Civil Procedure—including Rule 76a—rendered the proposed amendment unnecessary. TEX. CIV. PRAC. & REM. CODE § 134A.007(c) (“To the extent that this chapter conflicts with the Texas Rules of Civil Procedure, this chapter controls.”). Therefore, this provision was removed from the legislation.

#### **I. Effective Date**

These amendments to TUTSA went into effect on September 1, 2017.

### **III. TEXAS PATTERN JURY CHARGE ON TRADE SECRETS**

After TUTSA’s enactment in 2013, the Trade Secrets Committee and the Committee on Pattern Jury Charges spent two years considering and discussing the draft pattern charge for claims under TUTSA. The combined work of these two committees culminated in the pattern jury charge (PJC) for trade-secret misappropriation published for the first time in the 2016 edition of the *Texas Pattern Jury Charges for Business, Consumer, Insurance, and Employment*. The PJC includes questions and instructions on the existence of a trade secret (PJC 111.1), questions and instruction on trade-secret misappropriation (PJC 111.2), a question on trade-secret misappropriation damages (PJC 115.54), and sample instructions on actual damages on trade-secret misappropriation cases (PJC 115.55). In addition, the PJC includes detailed comments on when to use the trade-secret instructions and definitions, explanation of the elements of damage recoverable for trade-secret misappropriation, and commentary on the recovery of attorneys’ fees and exemplary damages.

Remember, though, the PJC was published before the TUTSA amendments were enacted so there might be slight variations between the PJC and the current version of TUTSA

#### **IV. RECENT DEVELOPMENTS IN TEXAS TRADE SECRETS CASE LAW**

##### **A. Anti-SLAPP Statute Applies to TUTSA Claims**

The Austin Court of Appeals recently issued a first of its kind opinion holding that the Texas Citizens Participation Act (TCPA)—also known as the Texas anti-SLAPP statute—can potentially be invoked to successfully defend against TUTSA claims. In *Elite Auto Body LLC, d/b/a Precision Auto Body v. Autocraft Bodywerks, Inc.*, 520 S.W.3d 191 (Tex. App.—Austin 2017 pet. filed), plaintiff sued its competitor and several former employees alleging that the employees provided its competitor with plaintiff’s trade secrets. In particular, Plaintiff alleged:

1. The former employees breached a fiduciary duty by misappropriating plaintiff’s trade secrets;
2. Defendants used plaintiff’s trade secrets;
3. Plaintiff’s former employees communicated plaintiff’s trade secret information to its competitor;
4. Defendants communicated with plaintiff’s current employees to induce them to leave plaintiff and work for defendant.

In response, defendant filed a motion to dismiss under the TCPA, in which it sought to establish by a preponderance of the evidence that (1) plaintiff asserted a legal action (2) based on, relating to, or is in response to (3) either the exercise of the right of association or the exercise of the right of free speech. Once defendant met this burden, plaintiff had to establish by clear and specific evidence a prima facie case for each element of its claims. Plaintiff, however, did not focus on presenting this evidence, choosing instead to argue that the TCPA did not apply. The trial court agreed with plaintiff and denied defendants’ motion to dismiss.

The Austin Court of Appeals reversed in part, focusing its analysis on the right of association. The right of association under the TCPA requires a “communication,” which includes the making or submitting of a statement or document in any form or medium, including oral, visual, written, audiovisual, or electronic. Because the first two allegations did not necessarily involve communications, the Austin Court held that the trial did not err in denying defendants’ TCPA motion.

But the Austin court found that the latter two allegations involved protected communications. The Austin court, applying the plain language of the statute, held that defendants met their burden of showing that plaintiff’s legal action (at least with respect to the latter two claims) was based on, related to, or is in response to defendants’ exercise of the right of association. Therefore, the Austin court concluded that the district court erred in failing to dismiss plaintiff’s latter two claims.

So what does this mean for TUTSA litigants? First, defendants have a new weapon—the TCPA—to use against plaintiffs. Second, plaintiffs must be especially careful not to base their TUTSA claims entirely on “communications,” as that term is defined in the TCPA. The problem, however, is that several of the paths to liability under TUTSA impose liability for disclosure of a

trade secret, and one cannot disclose a trade secret without some sort of communication. Thus, if a plaintiff's claim is based on disclosure of a trade secret to another party, then the plaintiff must be prepared to introduce clear and specific evidence of a prima facie case for each element of its claims or risk having its claims dismissed by the trial court.

Can TUTSA litigants escape the application of the TCPA by filing suit in federal court? According to the Southern District of Texas, the answer to this question is “no.” *Banik v. Tamez*, 7:16-CV-462, 2017 WL 1228498, at \*5 (S.D. Tex. Apr. 4, 2017); *La'Tiejira v. Facebook, Inc.*, CV H-16-2574, 2017 WL 3426039, at \*1 (S.D. Tex. Aug. 7, 2017) (holding that “[a]lthough the TCPA is a state law, it applies to Texas law claims in a federal court sitting in diversity”). Although parties have argued that the TCPA's procedural rules should not apply in federal court, the Fifth Circuit has yet to consider such issue. *See Cuba v. Pylant*, 814 F.3d 701, 706 n.6 (5th Cir. 2016) (stating that “we assume, without deciding, that the state procedural rules . . . do in fact apply in federal court”). Accordingly, if a trade-secret plaintiff's claim relates in part to “communications” and they wish to avoid the application of the TCPA, at least for now, the Plaintiff will need to sue in federal court under DTSA rather than under TUTSA.

### **B. “Attorneys’ Eyes Only” Does Not Always Mean “Attorneys’ Eyes Only”**

Often, in trade secrets and other types of commercial litigation, the courts will enter protective orders so that the parties can exchange trade secret or proprietary information without losing the “secret” nature of the information. This exchange of information is generally necessary so that the parties can understand the nature of the dispute. For instance, if the claim is that a competitor misappropriated a customer list, the plaintiff might have to produce the customer list that it claims was misappropriated. Additionally, the parties often exchange confidential financial information in order to prove their damages.

The court's protective order protects this exchange of information by placing limits on who can see the information, how many copies can be made of the information, or how the information can be used in open court or at deposition. The degree of these restrictions often depends on whether the information is classified as “Confidential” or as “Confidential – Attorneys’ Eyes Only.” “Confidential – Attorneys’ Eyes Only” information generally has the most restrictions. This designation typically means that only the attorneys or retained experts can view the information and not the parties themselves. It is generally reserved for the most sensitive information in the case.

However, in *In re Commercial Metal Company*, No. 05-16-01214-CV, 2017 WL 3712169 (Tex. App.—Dallas Aug. 29, 2017, no pet. h.), the Fifth Court of Appeals acknowledged that sometimes “Attorneys’ Eyes Only” doesn't always mean “Attorneys’ Eyes Only.” In *In re Commercial Metal Company*, the trial court entered a protective order that allowed “Attorneys’ Eyes Only” information to be disclosed not only to litigation counsel but also to the three in-house counsel of the defendant. Plaintiff, however, did not have any in-house counsel. The Court's order still allowed one of plaintiff's three owners to view the “Attorneys’ Eyes Only” information. Despite defendant's complaints, the Fifth Court of Appeals found that the protective order was an appropriate balancing of both parties' concerns because the owner was prohibited from participating in customer bids for a certain amount of time and because plaintiff was required to “place reasonable protections and restrictions so that no ‘Confidential—Attorney Eyes Only Material’ may be disseminated to anyone [else] at the company . . . .” *Id.* at 2.

### **C. When Customer Lists are Not Trade Secrets under TUTSA**

In *Baxter & Associates, L.L.C. v. D & D Elevators*, No. 05-16-00330-CV, 2017 WL 604043 (Tex. App.—Dallas Feb. 15, 2017, no pet.), Baxter Elevators argued that it was entitled to injunctive relief because its two former employees had misappropriated its customer lists. The trial court denied the relief because Baxter Elevator had an adequate legal remedy for the misappropriation. Baxter Elevators appealed, arguing that it was not required to prove that it did not have an adequate remedy at law. The Fifth Court of Appeals, however, never reached this issue because there was legally and factual sufficient evidence to support an implied finding that the alleged customer lists were not within the definition of a “trade secret” under TUTSA. First, the Court cited the following evidence that demonstrated that the customer lists did not derive independent economic value, actual or potential, from not 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:

- Defendant could not recall ever seeing a Baxter Elevator customer list while working there;
- Defendant found work by driving around “high-end” neighborhoods, contacting builders and architects, and advertising; and
- Defendant obtained information about certain customers by pulling their elevator permits.

Second, the Court cited the following evidence that demonstrated that the customer lists were not the subject of efforts that were reasonable under the circumstances to maintain their secrecy:

- Defendant worked for Baxter Elevators for six years before he was asked to sign any confidentiality agreement;
- Defendant representatives continued to work for Baxter Elevators after refusing to sign the confidentiality agreement;
- Baxter Elevators’ customer information data was not password protected, was not encrypted, and was not labeled confidential or proprietary.

Overall, *Baxter & Associates* provides an excellent analysis of a trade secret under TUTSA.

### **D. Court Muddies the Standard for Obtaining Injunctive Relief under TUTSA**

*Hughes v. Age Industries*, No. 04-16-00693, 2017 WL 943423 (Tex. App.—San Antonio March 8, 2017, no pet.) involves the familiar fact pattern of a key employee leaving his employer to work for a competing business. In addressing the employee’s argument that the employer failed to prove the existence of trade secret, the court stated that “[i]n the temporary injunction context, a trial court does not decide whether the information sought to be protected is a trade secret; rather it determines whether the applicant has established the information is entitled to trade secret protection until a trial on the merits.” This is an interesting comment because TUTSA makes no mention of this lesser standard in its language. Rather, the court relied on outdated common law case law as the basis for its statement. The effect of the court’s statement is to establish a possibly easier standard for establishing a plaintiff’s temporary injunction although it is not clear what the difference between “trade secret” and “information . . . entitled to trade secret protection until a trial on the merits” is.

The court further analyzed whether the employer had established a “probable, imminent, and irreparable injury,” which is the standard for common law injunctive relief but not the standard for TUTSA injunctive relief. Under TUTSA, “[a]ctual or threatened misappropriation may be enjoined.” Not only does TUTSA not mention requiring a “probable, imminent, and irreparable injury,” it states that damages for misappropriation can be “in addition” to injunctive relief, implying that proof of a probable, imminent, and irreparable injury—i.e., an injury that “cannot adequately compensated in damages” or “cannot be measured by any certain pecuniary standard”—is not a requirement of TUTSA. Again, the Court’s analysis seems to mix Texas trade secret common law with TUTSA for an interpretation that is not necessarily consistent with the statute.

#### **E. “Use” of a Trade Secret Can be Inferred in Certain Situations**

In *RealPage, Inc. v. Enterprise Risk Control, LLC*, 4:16-CV-00737, 2017 WL 3313729 (E.D. Tex. Aug. 3, 2017), the trial court granted a temporary injunction to the plaintiff who alleged its former employee was using its trade-secret information. Defendant argued that plaintiff was not entitled to trade secret protection because its alleged trade-secret information could be easily learned by any member of the public and that plaintiff did not act diligently in protecting its trade secrets. *Id.* at \*9.

In rejecting this contention, the court observed that plaintiff did adequately protect its trade secret information through “confidentiality agreements, login credentials, passwords, firewalls, and requiring return of information upon termination.” *Id.* at 10. Additionally, plaintiff sent a cease and desist letter to defendant when it first learned of a potential breach of confidentiality by defendant.

Defendant further argued that plaintiff had no evidence that defendant was using the alleged trade-secret information. Although plaintiff had little evidence of actual use, it argued that “use” can be implied from defendant’s quick development of its own software code that was similar to plaintiff’s. *Id.* at 11.

In analyzing these arguments, the court first observed that any exploitation of a trade secret that is likely to result in injury to the trade secret owner or enrichment of the defendant is a “use.” *Id.* Accordingly, “use” can be found where the exploitation includes “relying on the trade secret to assist or accelerate research or development.” *Id.* (quoting *GlobeRanger Corp. v. Software AG United States of Am., Inc.*, 836 F.3d 477, 498 (5th Cir. 2016)). According to the court, an inference of use by the defendant may be justified when the plaintiff can establish a defendant’s knowledge of the trade secret combined with substantial similarities between the parties’ products. *Id.* (citing *Spear Mktg., Inc. v. BancorpSouth Bank*, 791 F.3d 586, 601 (5th Cir. 2015)). Thus, a factfinder may find use by the defendant when “the defendant’s product was quickly developed by someone who had recently resigned from the plaintiff-company.” *Id.* (quoting *Aspen Tech., Inc. v. M3 Tech., Inc.*, 569 Fed. App’x 259, 267 (5th Cir. 2014)).

Although former employees are entitled to use general knowledge gained from their former employee, they are not entitled to use specific information they learned through their former employment. *Id.* at \*14. The court, therefore, concluded that plaintiff was being irreparably harmed by defendants’ misappropriation because defendants could improve on plaintiff’s trade secrets without first investing the time, expense, and labor necessary to produce a duplicate product. *Id.* The court further found that “[a]ny calculation of monetary damages would fail to fully appreciate the harm done by defendants developing a robust product by skipping the necessary research and development undertaken by every other competitor.” *Id.*



## **F. Information Not Entitled to Trade-Secret Status if the Owner Fails to Take Any Affirmative Steps to Preserve its Secrecy**

In *BCOWW Holdings, LLC v. Collins*, SA-17-CA-00379-FB, 2017 WL 3868184 (W.D. Tex. Sept. 5, 2017), the district court denied injunctive relief to the plaintiff who alleged its former employee was using its trade-secret information. Plaintiff alleged that defendant misappropriated, among other things, its confidential drawings (engineering plans), pricing information, and customer and vendor information. *Id.* at \*14.

Regarding the vendor information, the court observed that vendor lists can be trade secrets, but plaintiff failed to present any evidence that defendant had taken and was working from a list or compilation of vendor information. *Id.* Plaintiff also argued even if it did not maintain a list of customers or vendors, the names of its customer and vendor contacts qualified as trade secrets because defendant learned this contact information through his employment with plaintiff. *Id.* In rejecting this argument, the court determined that plaintiff had not taken any steps to protect the contact information of its vendors and customers, and that most of the contacts could be found on the internet. *Id.* Accordingly, because plaintiff took no steps to preserve the secrecy of such information, the mere fact that its former employees learned the vendor contact information from plaintiff does not render non-secret information a secret. *Id.*

Regarding the customer information, the court held that “[c]ustomer relationships do not qualify as trade secrets just because a company invests time and money to cultivate those relationships.” *Id.* at 15. According to the court, “TUTSA protects an employer’s secrets, not its relationships.” *Id.* The court reasoned that this is why many employers insist upon non-compete agreements: to protect their goodwill and to prohibit former employees from being able to take advantage of that time and investment to their detriment. *Id.*

As for Plaintiff’s engineering drawings and price information, the court observed that these are certainly protected by TUTSA—if the information is kept a secret. Relying on pre-TUTSA authority, plaintiff argued that it took reasonable efforts to maintain the secrecy of its information by only disclosing it to persons under an implied obligation not to use or disclose it and only on a limited basis. *Id.* at 16. The court found plaintiff’s citation to pre-TUTSA authority unpersuasive because TUTSA requires that *affirmative* steps be taken to preserve the secrecy of information to qualify for trade secret information. *Id.* Reasonable efforts to maintain the secrecy of information may include advising employees of the existence of a trade secret, limiting disclosure on a need-to-know basis, having employees or third parties sign non-disclosure agreements, encrypting data files, and marking files as confidential. *Id.* at 15. Because plaintiff took *none* of these steps to protect the secrecy or confidentiality of its information, the court found that it was not entitled to trade secret protection. *Id.* at 16.

Under the court’s analysis, an employer must take *some* steps to preserve the secrecy of its information. What is unclear, however, is how much effort an employer must take to protect the secrecy of its information. Courts obviously will consider an employer’s efforts on a case-by-case basis to determine if the steps taken to preserve secrecy were reasonable under the circumstances. Accordingly, if an employer takes at least some steps to maintain the secrecy of its information, it may be able to protect its information as a trade secret under TUTSA. Additionally, if a particular employer places particular value on the relationships it has made with its customers and vendors, this court’s holding indicates that such relationships are not protectible under TUTSA, and employers should enter into non-competition agreements with its employees.

## V. TUTSA BUSINESS FORMS

Because it is important that trade secret owners take reasonable precautions to prevent the disclosure of their trade secrets, the authors have included an appendix with forms that can serve as guidelines to be used in drafting provisions aimed at protecting your client's valuable trade-secret information. In particular, your clients' forms should be updated to reflect mandatory disclosure requirements found in the federal Defend Trade Secrets Act. With the enactment of DTSA, "any contract or agreement with an employee that governs the use of trade secret or other confidential information" is expected to provide notice of certain trade secret disclosure immunities to employees, contractors, or consultants. 18 U.S.C. § 1833 (2017). This immunity provision applies when an employee, contractor, or consultant: (1) discloses a trade secret in confidence to a federal, state, or local official for the purpose of reporting or investigating a suspected violation of law, or (2) discloses a trade secret in a complaint or other document filed in a lawsuit under seal. *Id.* It also applies in certain situations in anti-retaliation lawsuits. *Id.* If an employer fails to include this notice in its trade secret agreements, the employer will lose the right to recover exemplary damages or attorneys' fees in subsequent DTSA suits against individuals who did not receive the notice. *Id.* Thus, companies who are considering using the DTSA as a possible weapon against misappropriation should include a DTSA notification clause in their non-disclosure agreements.

**Joseph F. Cleveland, Jr., J. Heath Coffman, and Jared Wilkinson** practice in the areas of intellectual property and commercial litigation at Brackett & Ellis, PC. Mr. Coffman is the chair—and Mr. Cleveland is the past chair—of the Trade Secrets Committee of the Intellectual Property Section of the State Bar of Texas. Mr. Cleveland and Mr. Coffman were both members of the working group responsible for drafting TUTSA and its amendments and assisting in the preparation of the bill analysis for the Senate and House committees. Mr. Coffman frequently blogs about trade secrets and other intellectual property and commercial litigation matters at [fwlawreporter.com](http://fwlawreporter.com).

**APPENDIX**

<b>Tab</b>	<b>Description</b>
A	Termination Return of Property Checklist
B	“Confidential Information and Company Property” Employee Handbook Provision
C	Cease and Desist Letter
D	Non-Disclosure, Non-Solicitation and Non-Competition Agreement

# TAB A

## Termination Return of Property Checklist

I, [name of Employee], represent that I have returned **all** property belonging to my former employer, [name of Employer], to the custody of Employer's President [or other Company Representative], effective [date].

1. I acknowledge that I received, read, and signed [employee manual] at the commencement of my employment with [Employer].

2. I acknowledge that while employed at [Employer] I had access to [Employer's] confidential information and I will not disclose that confidential information to others.

3. I understand that "property belonging to Employer" includes, but is not limited to, the following specific items. I have placed a check-mark beside each item that I have returned to [name of Employer]: [include all applicable items]

- Building keys \_\_\_\_\_
- Desk keys \_\_\_\_\_
- Mailbox keys \_\_\_\_\_
- Card keys \_\_\_\_\_
- Electronic access keys or other devices \_\_\_\_\_
- Computer discs \_\_\_\_\_
- Electronic data stored in any medium (e.g., discs, hard drive memory, thumb drive, cds, tapes, cards, etc.) \_\_\_\_\_
- Company credit cards \_\_\_\_\_
- Company cell phone \_\_\_\_\_
- Company computer equipment \_\_\_\_\_
- Customer lists any other customer information \_\_\_\_\_
- Designs or formulas \_\_\_\_\_
- Price lists \_\_\_\_\_
- All company files \_\_\_\_\_
- Company financial information \_\_\_\_\_
- Company manuals \_\_\_\_\_
- Other Company property (specify any additional applicable property) \_\_\_\_\_

4. I have not made and/or kept a copy or copies of any documents, printed material, electronic data however stored (e.g, discs, hard drive memory, thumb drive, cd, tape, etc.) or other company information made available to me, provided to me or to which I had access, while an employee of [name of Employer].

5. I have not retained and/or not made a copy or copies of any customer job orders, files, lists, information concerning the company's operational methods, sales techniques, billing rates, price lists, cost data, order guides, customer preferences and buying patterns or any other statistical data, forms, files, records, documents or any similar items of information relating to [Employer's business].

6. I acknowledge that I executed [name any non-competition, non-solicitation, or non-disclosure agreements] at the commencement of my employment with [Employer], and that I have continuing duties under such [name agreement(s)] subsequent to my departure from [Employer].

7. I acknowledge that [Employer] expects full compliance with, and will enforce, all contractual and common law duties owed to [Employer].

I declare under penalty of perjury that the foregoing statements are true and correct.

_____ Name of Employee	_____ Signature	_____ Date
_____ Name of Employee	_____ Signature	_____ Date

# TAB B

## **Confidential Information and Company Property**

During your employment by [Employer], you may have access to confidential and proprietary data which is not known generally by competitors within the [describe industry]. This information (hereinafter referred to as “Confidential Information”) includes, but is not limited to, [specifically list Company’s confidential information. Determine what type of information and communication Company intends to prohibit the disclosure and use of, and draft the provision that specifically identifies items without using broad and ambiguous descriptions or categories of information. Additionally, do not over-designate what Company considers to be confidential information.] [Items could include: data relating to the company’s marketing and servicing programs, procedures and techniques; the criteria and formulae used by the company in pricing its products and services; the structure and pricing of special packages that the company has negotiated; lists of customers and prospects; the identity, authority, and responsibilities of key contacts at company accounts; the composition and organization of accounts’ businesses; the peculiar risks inherent in their operations; sensitive details concerning the structure, conditions, and extent of their existing products and services; contract expiration dates; commission rates; service arrangements; computers/hardware, proprietary software, web applications and analysis tools; and other data showing the particularized requirements and preferences of the accounts.] This Confidential Information constitutes a valuable asset of the Company, developed over a long period of time and at substantial expense. All Confidential Information should be safeguarded and any release duplication, distribution, transmittal, disclosure, or discussion (“release”) of such information that is not required by law or by the duties of the employees involved is strictly prohibited.

Unauthorized access to, and unauthorized release of, Confidential Information will violate this policy and may result in appropriate disciplinary action against the employee(s) involved, up to and potentially including termination of employment, depending on the severity and/or repeat nature of the offense.

To protect the Company’s interest in this valuable asset, you must (a) not use any such Confidential Information for your personal benefit or for the benefit of any person or entity other than the Company, (b) not disclose any such Confidential Information to any person or entity outside the Company under any circumstances without written permission, and (c) use your best efforts to limit access to such Confidential Information to those who have a need to know it for the business purposes of the Company.

In addition, you should minimize those occasions on which you take Company laptops, electronic equipment, documents, hard drives, flash drives or any other electronic medium containing Confidential Information outside the office. On those occasions where it is necessary, consistent with the best interests of the Company and doing your job effectively, to take any of these items containing Confidential Information outside the office, all appropriate precautionary and security measures should be taken to protect the confidentiality of the information.

During the course of your employment with the Company, you will be provided and/or will generate correspondence, memoranda, literature, reports, summaries, manuals, proposals, contracts, customer lists, prospect lists, and other documents and data concerning the business of the Company. Any and all such records and data, whether maintained in hard copy or on a computer disk, computer hard drive, flash drive, or other medium is the property of the Company,



regardless of whether it is or contains Confidential Information. Upon termination of your employment at the Company, you are required to return all such records to the Company and may not retain any copy of any such records or make any notes regarding any such records. The Company retains the right to access all Company property including computers, desks, file cabinets, storage facilities, and files and folders, electronic or otherwise, at any time. Employees should not entertain any expectation of privacy when on Company grounds or while using Company property.

**NOTICE:** An individual shall not be held criminally or civilly liable under any Federal or State trade secret law for the disclosure of a trade secret that is made in confidence to a Federal, State, or local government official or to an attorney solely for the purpose of reporting or investigating a suspected violation of law. An individual shall not be held criminally or civilly liable under any Federal or State trade secret law for the disclosure of a trade secret that is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal. An individual who files a lawsuit for retaliation by an employer for reporting a suspected violation of law may disclose the trade secret to the attorney of the individual and use the trade secret information in the court proceeding if the individual files any document containing the trade secret under seal and does not disclose the trade secret, except pursuant to court order.

# TAB C

[Date]

[Former Employee]  
[Address]

Re: Cease & Desist Notice | [Company]

Dear [Former Employee]:

Please be advised that I have been retained to represent [Company] with respect to your recent resignation from [Company] and, more specifically, protection of [Company's] property and confidential information. It has come to our attention that you have [describe wrongful conduct, for example: forwarded [Company] electronic information and documents to your personal email account in violation of [Company Employee Manual] and [Non-Disclosure Agreement]] which you executed at the outset of your employment with Company ("the Agreement"). For your convenience, I have enclosed a copy of the Agreement.

Specifically, you agreed, among other things, not to use [Company's] trade secrets, customer and other confidential data on your own behalf or disclose such information to any third-party except in furtherance of your employment at [Company] and as an employee of [Company]. At termination, you were reminded of your legal obligations and further instructed to return all [Company] property, including any paper and/or electronic files of [Company's] customers.

Per the Agreement, Confidential Information includes, but is not limited to, any information of a technical, financial or business nature with respect to [Company] or its business, whether or not marked confidential, which is not published or readily available to the public, and includes customer lists and information. By forwarding [Company's] electronic information and documents to your personal email account, you have breached the Agreement.

Your continued possession of [Company's] documents and customer information in your personal email or elsewhere is in direct violation of the Agreement and may also violate other federal and state laws designed to protect [Company's] property and Confidential Information.

[Company] therefore demands that you: [include all that apply]

1. Immediately return to [Company] any materials, including electronic files in your possession or control and whether on your laptop or other electronic devices, that could be characterized as trade secret or Confidential Information, as defined on Page \_\_ of the Agreement;
2. Immediately return to [Company] all files and documents, whether electronic or physical, and all client information, including any contact information or information pertaining to particular needs and requirements of [Company] customers which you obtained during your employment with [Company];

3. Immediately return to [Company] all trade secrets, customer data, and any other [Company] confidential data that you downloaded to any USB flash drive or other portable storage device or emailed to yourself and within your possession or control;
4. Immediately cease and desist from any further use of, either for yourself or the benefit of others, the trade secrets, customer data or other confidential data in your possession or elsewhere;
5. Immediately cease and desist any indirect or direct disclosure of any trade secrets, customer data, or other confidential information to anyone for any reason;
6. Immediately cease and desist revealing, directly or indirectly, the description of trade secrets, customer data, or other confidential data, including but not limited to the identity of a customer or customer contact information, to your prospective employer or anyone;
7. Immediately cease and desist any direct or indirect contact, calls, communications with, attempts to communicate with, solicitation or acceptance of business from any [Company] Customer, as defined in the Agreement; and
8. Immediately furnish a copy of the Agreement to your prospective employer as you are obligated to do pursuant to Page \_\_ of the Agreement and provide written confirmation to [Company] that you have fully complied with this obligation.

You may make arrangements for the return of those materials identified in Items 1-3, above, by contacting [Company Employee] at [phone number] or [email [address](#)] no later than **[time, day, date]**.

Because you have already breached your Agreement with [Company], [Company] further demands that you verify in writing, no later than **[time, day, date]**, the destruction or return of any and all of [Company's] property and confidential information, whether electronic or physical copies, from your possession. Additionally, to protect [Company's] legitimate business interests, [Company] demands that you provide, at your expense and **no later than \_\_\_\_\_ on \_\_\_\_\_, \_\_, 2017**, written confirmation to [Company] from a licensed, forensic investigator that any and all of [Company's] property and Confidential Information has been removed in its entirety from your personal email account and computer. You are specifically advised that any failure or delay in complying with these demands will likely compound the damages for which you may be liable. You are further advised that, pursuant to Tex. Civ. Prac. & Rem. Code § 38.001, attorney's fees are recoverable for the breach of a contract.

If [Company] has not received **full compliance with the above demands by the close of business on [day, date]**, [Company] is prepared to take all necessary steps, including suit to enjoin your continued violations, to protect its rights, pursuant to your agreements with [Company], without further notice to you. In addition to injunctive relief, [Company] will seek monetary damages and all costs or expenses, including attorneys' fees, incurred in enforcing this Agreement due to your violations. If you fail to comply with your duty to provide the Agreement to your future employer and provide satisfactory written confirmation to [Company] of such compliance, [Company] will exercise its right to do so pursuant to Page \_ of the Agreement.

The above is not an exhaustive statement of the relevant facts and law. [Company] expressly reserves all of its legal and equitable rights and remedies, including the right to seek injunctive relief and recover monetary damages, costs, and attorney's fees.

[Company] trusts, moving forward, that you will honor your legal obligations, including those set forth in the Agreement. If you have any questions or concerns regarding this correspondence or your obligations to [Company], please contact me. If you are represented by legal counsel, please have your attorney direct any questions or concerns to me.

Sincerely,

[Name of Attorney]

# TAB D

**NON-DISCLOSURE, NON-SOLICITATION  
AND NON-COMPETITION AGREEMENT**

This Non-Disclosure, Non-Solicitation and Non-Competition Agreement (the “Agreement”) is made and entered into on this \_\_\_\_ day of \_\_\_\_\_, 2017, by and between [Employer Name], a Texas [Entity Type] (“Employer”) and \_\_\_\_\_ (“Employee”).

WITNESSETH:

WHEREAS, Employer is engaged in the business of [describe Company’s business]; and

WHEREAS, Employer desires to employ Employee as an [position] and Employee desires to seek employment with Employer; and

WHEREAS, Employer will expend resources in training Employee and will provide Confidential Information (as defined below) to Employee; and

WHEREAS, Employee’s duties to Employer as [position] will include, among other things, [list duties, for example: interacting with Employer’s Customers, (as defined below), establishing relationships with Prospective Customers (as defined below), providing Employer’s products and services to Employer’s Customers, and managing Employer’s relationships with Employer’s Customers and Prospective Customers]; and

WHEREAS, Employee will play an important role as [position] in the development and maintenance of Employer’s Confidential Information and goodwill on behalf of Employer;

WHEREAS, as a condition precedent to employment with Employer, Employer requires Employee, and Employee has agreed, to enter into and execute this Agreement; and

WHEREAS, Employee agrees that the protections in this Agreement are reasonable and necessary to ensure that the confidentiality of Employer’s Confidential Information (as defined below) is adequately protected and that the goodwill Employer has developed in the relevant market is not damaged or compromised.

NOW THEREFORE, FOR VALUABLE CONSIDERATION, including but not limited to employment, continued employment; compensation; promotion; unique, extraordinary, and specialized development and training; access to certain of Employer’s Confidential Information, trade secrets and other proprietary information; and substantial knowledge of and relationships with Customers, the receipt and sufficiency of which is acknowledged, Employee agrees with Employer as follows:

1. **Definitions.** Whenever used in this Agreement, the following terms shall have the following respective meanings:

- (A) **“Confidential Information”** means each, every, and all written documentation (in whatever form stored), relating to or evidencing Employer’s:

- i. Records and lists of Employer's Customers and Prospective Customers (as defined below);
  - ii. Accounts and records pertaining to Employer's Customers and Prospective Customers (as defined below) and suppliers;
  - iii. Programs, systems, processes and other products and/or services designed for Employer's customers;
  - iv. Schedules of fees or charges for Employer's products and services;
  - v. Financial information of the company, business plans and business strategies;
  - vi. Advertising or marketing plans and market studies;
  - vii. Goals, objectives and projections;
  - viii. Personnel information;
  - ix. Business practices, including, without limitation, Employer's proprietary sales practices and techniques;
  - x. Work product that is generated, developed, or obtained by any employee, including Employee, of Employer during the course and scope of such employee's employment with Employer;
  - xi. Computer software and programs; and
  - xii. Any other information known by Employee to be considered proprietary or maintained in confidence by Employer.
- (B) "Employer's Business" means [define Company's Business] and all development, programming, marketing, solicitation, and other routine practices incidental to such business operations.
- (C) "Directly or Indirectly" means to do an act oneself or to assist another person or entity in doing an act.
- (D) "Compete" means to means (1) to perform or attempt to perform tasks or duties on behalf or at the direction of a Competitor (as defined below) that are substantially similar to the tasks or duties Employee performs on behalf or at the direction of Employer, or (2) to perform or attempt to perform exclusively for the pecuniary benefit of Employee tasks or duties that are substantially similar to the tasks or duties Employee performs on behalf or at the direction of Employer.
- (E) "Employer's Customers" means the persons or entities that are identified as customers of Employer in any written or electronic records of Employer.



- (F) “Competitor” means any person, firm, corporation, association or other form of entity that engages in Employer’s Business.
- (G) “Market Area” means that geographic area that is within thirty (30) miles of the city limits of [Address] (Employer’s current place of business) or Employer’s place of business at the time of Employee’s termination from employment with Employer.
- (H) “Customer’s Market Area” means the geographic area that is within a one (1) mile radius of Employer’s Customer’s or Employer’s Prospective Customer’s principal place of business or Employer’s Customer’s place of business in which the Employee conducted Employer’s Business with Employer’s Customers or Prospective Customers while employed by Employer.
- (I) “Prospective Customer” means any person or entity to whom Employer makes business proposals with Employee’s participation during Employee’s employment with Employer.

2. **Non-Disclosure of Confidential Information.** Employer agrees to provide to Employee some or all of the Confidential Information. Employee acknowledges that the Confidential Information constitutes valuable, secret, special, and unique assets of Employer. Employee agrees that Employee will not disclose the Confidential Information to any person or entity for any reason or purpose without the express written approval of Employer, and will not use the Confidential Information except in furtherance of Employee’s duties to Employer. In the event the laws of the State applicable to the enforcement of this Paragraph impose a reasonable time limitation, the period shall be deemed to be the term of Employee’s employment with Employer and for twenty-four (24) months thereafter.

3. **Ownership and Return of Confidential Information.** Any Confidential Information that is furnished to Employee by Employer, used by Employee on Employer’s behalf, or generated, developed, or obtained by Employee during the course of Employee’s employment with Employer, shall be and remain the property of Employer. Employee acknowledges that this information is confidential and is not readily accessible to Employer’s Competitors, and Employee agrees to undertake reasonable measures to safeguard the secrecy of the information. Measures to safeguard the secrecy of Confidential Information shall be considered “reasonable” if they are at least commensurate with those measures that a reasonably prudent business person would undertake under the same or similar circumstances. Upon termination of Employee’s engagement with Employer, Employee shall immediately deliver to Employer or its authorized representative all Confidential Information, including physical and electronic copies, remaining in Employee’s possession, custody, or control.

4. **Ownership of Intellectual Property.** The parties agree that all patents, copyrights, or trademarks relating to any work product Employee develops or participates in developing in the course and scope of his duties to Employer shall be the sole and exclusive property of Employer. Employee agrees to cooperate with Employer and to execute such documents as are reasonably necessary to effectuate Employee’s assignment of his rights to any such patents, copyrights, or trademarks to Employer. Employee further agrees to assist Employer in every reasonable way in

any lawsuits Employer files against third parties to enforce its rights under any such patents, copyrights or trademarks. Employee's obligations under this paragraph shall survive termination of Employee's engagement with Employer. Upon termination of Employee's engagement with Employer, Employee shall immediately deliver to Employer or its authorized representative all of Employer's Intellectual Property, including physical and electronic copies, remaining in Employee's possession, custody, or control.

5. **Non-Solicitation of Employer's Customers.** Beginning on the date of execution of this Agreement and continuing for a period ending two (2) years following the termination (whether voluntary or involuntary) of Employee's employment with Employer, Employee agrees not to Directly or Indirectly conduct Employer's Business within the Market Area with any of Employer's Customers or Prospective Customers for the benefit of Employee or for the benefit of any Competitor.

6. **Agreement Not to Compete.** Beginning on the date of execution of this Agreement and continuing for a period of one (1) year following the termination (whether voluntary or involuntary) of Employee's employment with Employer, Employee agrees not to Directly or Indirectly Compete with Employer within the Market Area. Employee also agrees that during Employee's employment with Employer, Employee will not engage in any activities in furtherance of any intention of Employee to Directly or Indirectly Compete with Employer.

7. **Statutory Enforcement.** The covenants contained in Paragraphs 5 & 6 above are entered into between Employer and Employee with express reference to 15.50 - 15.52, Texas Business and Commerce Code, as now existing or hereafter amended. Employer and Employee intend for the covenants to be enforceable under those statutory provisions, and if any provision of the Agreement is determined by a court of competent jurisdiction to be void, illegal or unenforceable, in whole or in part, all other provisions will remain in full force and effect, as if the void, illegal, or unenforceable provision is not part of the Agreement. Employee agrees that the restrictions imposed upon Employee and the rights and remedies conferred upon Employer are: reasonable in time, territory and scope and designed to eliminate competition which would otherwise be unfair to Employer, are fully required to protect the legitimate business interests of Employer, and do not confer a benefit upon Employer disproportionate to the detriment of Employee.

8. **Termination of Employment with Employer.** Upon termination of Employee's employment or business relationship with Employer, Employee agrees and understands that the obligations set forth in this Agreement will survive.

9. **Conflicting Obligations and Rights.** Employee agrees to inform Employer in writing on Exhibit A-1 hereto of any apparent conflict between Employee's work for Employer and any obligations Employee may have to preserve the confidentiality of another's proprietary information or materials. Otherwise, Employer may conclude that no such conflict exists and Employee agrees thereafter to make no such claim against Employer.

10. **Subsequent Employment of Employee.** Employee agrees that prior to accepting any employment by, or association with a Competitor, Employee will notify any such Competitor of the existence and terms of this Agreement, and shall furnish such person or entity with a copy

of this Agreement. Upon request by Employee or the Competitor, Employer will provide a copy of this Agreement to the Competitor.

11. **Non-Solicitation of Other Employees.** Beginning on the date of execution of this Agreement and continuing for a period ending two (2) years following termination (whether voluntary or involuntary) of Employee's employment with Employer, Employee agrees not to Directly or Indirectly solicit or hire any of Employer's employees to work for (a) Employee in the Employer's Business or (b) for a Competitor.

12. **Disclosure of this Agreement.** Employee agrees that Employer may communicate the terms of this Agreement to any of Employer's Customers or Prospective Customers or to any Competitor if Employer reasonably believes Employee is engaged in conduct that could be a breach of this Agreement or if such Customer, Prospective Customer, or Competitor inquires as to the existence of this Agreement; and Employer shall incur no liability to Employee by reason of disclosure of the terms of this Agreement to any person to whom disclosure is authorized by this paragraph.

13. **Tolling.** Employee agrees that during any period in which Employee is in breach of the covenants contained in these Paragraphs 5, 6 and 11, the time period of such covenants shall be extended for an amount of time equal to the period in which Employee is in breach thereof. Employee further acknowledges and agrees that if Employee violates any covenant contained in these Paragraphs 5, 6 and 11 and Employer brings legal action for injunctive or other relief, Employer shall not, as a result of the time involved in obtaining the relief through litigation, be deprived of the benefit of the full period of any covenant. Accordingly, the covenants of Employee contained in these Paragraphs 5, 6 and 11 shall be deemed to have duration as specified above, which periods shall commence upon the later of (i) the ending date above stated or (ii) the date of entry by a court of competent jurisdiction of a final judgment enforcing the covenants of Employee set forth in these Paragraphs 5, 6 and 11.

14. **Breach of this Agreement.** In the event of breach of any of the provisions of this Agreement, Employer shall be entitled to injunctive relief as well as any other applicable remedies at law or in equity. Employee acknowledges that in the event of a breach of this Agreement by Employee, monetary damages alone would be inadequate to compensate Employer. This Agreement shall inure to the benefit of any successor in interest of Employer by way of merger, consolidation, or other similar succession.

15. **Identical Counterparts.** This Agreement may be executed in a number of identical counterparts, each of which shall be deemed an original for all purposes and all of which shall be construed together as comprising a single document.

16. **Waiver/Modification.** No waiver or modification of this Agreement shall be valid unless in writing and duly executed by Employer.

17. **Attorneys' Fees.** If any litigation arises to enforce or construe this Agreement, the prevailing party shall be entitled to an award of reasonable attorneys' fees, and costs. In the event a court enforces this Agreement, whether as written or as reformed by the Court, the Employer shall be deemed the prevailing party for purposes of this section.

18. **Entire Agreement.** This Agreement contains the entire agreement between the parties. Any prior agreement between the parties with respect to the subject matter of this Agreement shall be of no further force and effect.

19. **Severability.** Should any term or provision of this Agreement be declared invalid by a court of competent jurisdiction, the parties agree that all other terms of this Agreement are binding and have full force and effect as if the invalid portion has not been included.

20. **Choice of Law/Choice of Venue.** This Agreement shall be interpreted in accordance with the laws of the State of Texas and venue for any action in a court of law or equity respecting any aspect of this Agreement will be exclusively in \_\_\_\_\_ County, Texas.

21. **Survivability.** This Agreement shall be binding upon and inure to the benefit of the parties, and their respective personal representatives, heirs, successors, and assigns.

22. **Notices.** Unless a party provides written notice of an alternative address or e-mail address, any notices required or permitted to be given under this Agreement shall be sufficient if in writing and if sent by certified mail, hand-delivery, or electronically to:

23. **Defend Trade Secrets Act Notice:** An individual shall not be held criminally or civilly liable under any Federal or State trade secret law for the disclosure of a trade secret that is made in confidence to a Federal, State, or local government official or to an attorney solely for the purpose of reporting or investigating a suspected violation of law. An individual shall not be held criminally or civilly liable under any Federal or State trade secret law for the disclosure of a trade secret that is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal. An individual who files a lawsuit for retaliation by an employer for reporting a suspected violation of law may disclose the trade secret to the attorney of the individual and use the trade secret information in the court proceeding if the individual files any document containing the trade secret under seal and does not disclose the trade secret, except pursuant to court order.

**For Employer**

**For Employee**

[Company Name]  
Attn: [Company Representative]  
[Address]  
[Email]

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

23. **Acknowledgment of Employee:** **EMPLOYEE HAS CAREFULLY CONSIDERED AND AGREES THAT THE PROVISIONS OF THIS AGREEMENT ARE FAIR, REASONABLE, AND NOT UNDULY RESTRICTIVE ON EMPLOYEE, AND EMPLOYEE HAS HAD AN OPPORTUNITY TO OBTAIN LEGAL ADVICE BEFORE AGREEING TO THESE TERMS AND HAS ENTERED INTO THIS AGREEMENT VOLUNTARILY WITHOUT ANY DURESS OR COERCION.**

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the day and year first above written,

**[Company Name]**

**EMPLOYEE**

By: \_\_\_\_\_

Print Name: \_\_\_\_\_

Title: \_\_\_\_\_

**EXHIBIT A-1**

**NOTICE BY EMPLOYEE**

Please specify any obligations Employee may have to preserve the confidentiality of another's proprietary information or materials **here: (if none, please write "none" and initial bottom of page)**.