CONFIDENTIALITY CLAUSES – SCOPE AND EFFECTIVENESS

Mark J. Burzych
Fahey Schultz Burzych Rhodes, PLC
Okemos, Michigan

Nina Greene
Genovese Joblove & Battista, P.A.
Miami, Florida

October 10-12, 2018
Nashville, Tennessee

©2018 American Bar Association
# TABLE OF CONTENTS

I. **INTRODUCTION** ........................................................................................................................................... 1

II. **PROTECTION OF CONFIDENTIAL INFORMATION AS TRADE SECRETS** .................................................. 1
   A. Restatement Of Torts ................................................................................................................................. 2
   B. Uniform Trade Secrets Act ....................................................................................................................... 3
   C. Restatement (Third) Of Unfair Competition ........................................................................................... 6
   D. Defend Trade Secrets Act .......................................................................................................................... 6

III. **CONFIDENTIAL INFORMATION PROTECTION: 3 SCHOOLS OF THOUGHT** ............................................ 8
   A. Confidential Information Protectable Only If It Is A Trade Secret ............................................................ 8
   B. Confidential Information Is Protectable And Is Different From Trade Secrets ........................................ 16
   C. There Is A Difference Between Confidential Information And Trade Secrets And Only Trade Secrets Are Afforded Protection ........................................................................................................... 20

IV. **PRACTICE POINTERS** .................................................................................................................................. 23

V. **LITIGATING CONFIDENTIALITY CLAUSES IN FRANCHISE AGREEMENTS** .................................................. 28

VI. **CONCLUSION** ........................................................................................................................................... 34

Appendix 1

Biographies
I. INTRODUCTION

In the 1990s when the “create your own” restaurant trend was just beginning, ultimately leading to the creation of Qdoba, Chipotle, and similar concepts, the owner of a cutting edge “create your own” concept called with a problem. “A customer is sitting in the restaurant with a note pad drawing our floor plan. He’s counting ceiling tiles to get the measurements, and duplicating our floor plan! What can I do to stop him?!” the client asked.

Or what about the story that circled the internet a decade ago about Home Depot and Lowe’s, later debunked by Snopes.com.\(^1\) It was rumored that the jilted wife of the owner of the Home Depot used the knowledge she gained while in her marriage to create the competitive Lowe’s home improvement chain and located her stores next to the Home Depot stores in an effort to steal the Home Depot customers.

This is a typical situation in business. A business owner creates a new concept, nourishes it to market, only to have it get copied by others in the market. This situation happens frequently in the franchise industry. Franchisors design systems using confidential and proprietary information and license that confidential and proprietary information to franchisees who are under an obligation not to disclose that confidential and proprietary information to third parties. But what is “confidential” in a franchise system? Certainly the floor plan of a cutting edge “create your own” restauranteur or the “home improvement superstore” concepts are not confidential. The floor plan and the business concept are fully disclosed to the public and those businesses do not require customers to sign Confidentiality and Nondisclosure Agreements before being exposed to the design, floor plan, or business model. More important for franchisors is how to maintain the confidentiality of the keys to the business.

This paper will (i) summarize the various statutes that deal with the protection of confidential information as trade secrets; (ii) discuss generally how courts treat confidential information protection and three schools of thought that have evolved throughout the country;\(^2\) (iii) provide practice pointers for franchise practitioners; and (iv) discuss cases addressing confidentiality clauses and trade secrets in franchise agreements.

II. PROTECTION OF CONFIDENTIAL INFORMATION AS TRADE SECRETS

An initial question a franchise practitioner should ask is whether the franchisor’s confidential information is protected as a trade secret. To understand the interplay between confidential information and trade secrets, it is essential to understand what is meant by the term “trade secret.” Laws defining trade secrets vary from state to state, and thus, it is necessary to identify and confirm the definition of “trade secret” in the appropriate jurisdiction. For example, the Uniform Trade Secrets Act has been adopted in some form in almost all jurisdictions.\(^3\) The other remaining jurisdictions follow the Restatement of Torts or common law

\(^1\) Snopes.com (Lowe’s vs. Home Depot: Did the jilted wife of the owner of Home Depot create the Lowe’s chain of home improvement stores?) www.snopes.com/fact-check/the-lowes-down/

\(^2\) These schools of thought have been developed primarily in employment cases. However, these cases are nevertheless instructive to franchise practitioners in the area of confidential information protection.

definition of trade secret. The Restatement (Third) of Unfair Competition also addresses trade secret protection under the common law. In addition to state law, the Defend Trade Secrets Act creates a private right of action for the misappropriation of trade secrets under federal law. Each of these sources of law regarding the protection of trade secrets provides definitions of what constitutes a trade secret as further discussed below.

A. Restatement Of Torts

The definition of a “trade secret” was proscribed in the Restatement of Torts in 1939. Restatement of Torts § 757 sets forth a common law tort claim against a party that uses or discloses another’s trade secret without consent:

One who discloses or uses another’s trade secret, without a privilege to do so, is liable to the other if:

(a) he discovered the secret by improper means, or

(b) his disclosure or use constitutes a breach of confidence reposed in him by the other in disclosing the secret to him, or

(c) he learned the secret from a third person with notice of the facts that it was a secret and that the third person discovered it by improper means or that the third person’s disclosure of it was otherwise a breach of his duty to the other, or

(d) he learned the secret with notice of the facts that it was a secret and that its disclosure was made to him by mistake.

Comment (b) to Section 757 defines “trade secret” as “any formula, pattern, device or compilation of information which is used in one’s business, and which gives him an opportunity

---

4 See, e.g., Estee Lauder Companies Inc. v. Batra, 430 F. Supp. 2d 158, 175 (S.D.N.Y. 2006)(Under New York law, trade secrets are defined as set forth in the Restatement of Torts § 757, comment b (1939)).


6 RESTATEMENT (FIRST) OF TORTS § 757 (1939).
to obtain an advantage over competitors who do not know or use it. It may be a formula for a chemical compound, a process of manufacturing, treating or preserving materials, a pattern for a machine or other device, or a list of customers." The Restatement of Torts, a trade secret is a process or device for continuous use in the operation of the business.\(^7\)

The comments to Section 757 also require that "the subject matter of the trade secret be secret."\(^8\) Thus, matters that are generally known in an industry or of public knowledge are not trade secrets.\(^9\) However, an employer may disclose a trade secret to employees involved in using the information and are obligated by contract to keep the information confidential.\(^10\) Factors to be considered in whether a matter is trade secret under Section 757 are as follows:

(1) the extent to which the information is known outside of one's business;

(2) the extent to which the information is known by employees and others involved in the business;

(3) the extent of measures taken to guard the secrecy of the information;

(4) the value of the information to the owner and to competitors;

(5) the amount of effort or money expended in developing the information; and

(6) the ease or difficulty with which the information could be properly acquired or duplicated by others.\(^12\)

The rule stated in Section 757 protects the interest in a trade secret against both disclosure and adverse use.

B. **Uniform Trade Secrets Act**

The Uniform Trade Secret Act was promulgated in 1979 by the National Conference of Commissioners on Uniform State Laws. The Prefatory Note states that the "Uniform Act codifies the basic principles of common law trade secret protection."\(^13\) The Uniform Trade

---

7 Restatement (First) of Torts § 757, cmt. b (1939).

8 Id.

9 Id.

10 Id.

11 Id.

12 Id.

Secret Act provides the following definition for "trade secret":

"Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(i) derives 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, and

(ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.14

Courts have refined this definition of a trade secret as 'information that has independent economic value because it is not generally known or readily ascertainable and efforts are taken to maintain the information's secrecy.'15 The comments further set forth that the efforts required to maintain secrecy are those "reasonable under the circumstances."16 Courts do not require that extreme and expensive procedures be taken to protect trade secrets.17 While there is no precise definition of what is a reasonable effort to maintain the secrecy of a trade secret, the following, while not exhaustive, have been held to be reasonable efforts to maintain secrecy:

- controlled disclosure to employees and licensees;18
- limiting access to confidential information to individuals with a need to know;19
- limiting access to confidential information in computer systems to those with passwords;20 and
- signing confidentiality agreements or covenants.21

---

14 UTSA §1(4), (1985).


16 UTSA §1 cmt. (1985).


18 Stockade Cos., LLC v. Kelly Restaurant Group, LLC., No. 1:17-CV-143-RP, 2017 WL 4640443 at *5, n.4 (W.D. Tex. Oct. 16, 2017) (finding that where franchisor did not require franchisees to obtain confidentiality agreements from employees, which meant that any employee that left those franchisees could have put knowledge of the franchise system into public domain, franchisor did not limit access to confidential information).

19 Pyro Spectaculars N., Inc. v. Souza, 861 F. Supp. 2d 1079, 1090 (E.D. Cal. 2012) (court found the plaintiff exercised reasonable efforts to maintain secrecy where it required its employees to sign confidentiality agreements, maintain its confidential information remotely on secure network servers, required employees to use passwords with minimum complexity requirements to access the company database, and compartmentalized data and limited access by geographic region and job function).

20 See Cici Enters., L.P. v. Four Word Motion, LLC, 2016 WL 9244628, at *11 (reasonable efforts to maintain secrecy found where franchisor required franchisees to sign franchise agreements with confidentiality provisions).
To recover for misappropriation of trade secrets, a plaintiff must show a legally protectable secret, which was misappropriated by a defendant in violation of a confidential relationship. In determining whether a trade secret has been misappropriated under the Uniform Trade Secrets Act, actual or threatened misappropriation of trade secrets may be enjoined. The Act sets forth a three part inquiry:

The threshold inquiry is whether the information sought to be enjoined is indeed a legally protected trade secret ... the second element is whether an express or implied contractual or confidential relationship existed between the parties which obligates the party receiving the secret information not to disclose it; and finally, whether the party receiving the secret information wrongfully disclosed the information to the injury of the plaintiff.

The comments to the Uniform Trade Secret Act provide that "[o]ne of the broadly stated policies behind trade secret law is 'the maintenance of standards of commercial ethics.'" Under the Uniform Trade Secrets Act, a person or company may be liable for misappropriation of trade secrets in two different ways. A person or company may be liable for 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 disclosure or use of a trade secret of another without express or implied consent. The comment cites to Comment (f), in Section 757 of the Restatement of Torts, and notes: "A complete catalogue of improper means is not possible." However, Section 1(1) of the UTSA contains a partial listing of improper means, which includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means. Improper means could include otherwise lawful conduct which is improper under the circumstances; e.g., an airplane flight used as aerial reconnaissance to determine a competitor's plant layout during construction of the plant.

The comment also sets forth that proper means may include: discovery by independent invention; discovery by reverse engineering; discovery under a license from the owner of the trade secret; observation of the item in public use or on public display or obtaining the trade secret from published literature.

22 Id.
25 UTSA §1(4), cmt. (citing Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974)).
26 UTSA §1(1), cmt. (citing RESTATEMENT OF TORTS §757, cmt. F (1939)).
27 UTSA §1(1), cmt. (citing E.I. du Pont de Nemours & Co., 431 F.2d 1012).
28 UTSA §1(1), cmt.
C. **Restatement (Third) Of Unfair Competition**

The Restatement (Third) of Unfair Competition defines trade secret as:

"any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others."  

The comments to Section 39 of the Restatement (Third) of Unfair Competition make clear that the concept of "trade secret" as defined in the Restatement was intended to be consistent with the definition of "trade secret" in Section 1(4) of the Uniform Trade Secrets Act.  Accordingly, like the definition of "trade secret" adopted in the Uniform Trade Secrets Act, which does not include any requirement relating to the duration of the information's economic value, the definition adopted in Section 39 of the Restatement (Third) of Unfair Competition, and in contrast to the definition in the Restatement of Torts, contains no requirement that the information afford a continuous or long-term advantage.

With regard to value, the comments to the Restatement provide that a trade secret must be of sufficient value in the operation of a business to provide an actual or potential economic advantage over others who do not possess the information, but that the advantage need not be great. Value will be found if the trade secret provides an advantage that is more than trivial.

Information that is generally known or readily ascertainable through proper means by others to whom it has potential economic value is not protectable as a trade secret. Thus, information that is disclosed in published materials reasonably accessible to competitors or that is disclosed in the public domain does not qualify for protection under the Restatement. Likewise, information readily ascertainable from an examination of a product on public sale or display is not a trade secret.

D. **Defend Trade Secrets Act**

Effective May 11, 2016, the Defend Trade Secrets Act (the "DTSA") provides for a private right of action in Federal Court for civil seizure of "property necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action." The DTSA is

---


31 Id.

32 Id.

33 Id.


35 Id. at *4-5.

the first federal law to create a private right of action for the misappropriation of trade secrets.\textsuperscript{37} The DTSA includes definitions, remedies, and a statute of limitations substantially similar to provisions in the Uniform Trade Secrets Act.\textsuperscript{38} Although the Uniform Trade Secrets Act is effective in almost every state, those laws "vary in a number of ways and contain built-in limitations that make them not wholly effective in a national and global economy."\textsuperscript{39} The DTSA, however, is intended to provide a "single, national standard for trade secret misappropriation with clear rules and predictability for everyone involved."\textsuperscript{40}

Section 1836(b)(1) of the DTSA provides that "[a]n owner of a trade secret that is misappropriated may bring a civil action under this subsection if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." "In a civil action brought under [the DTSA] with respect to the misappropriation of a trade secret," the Court may award "damages for actual loss caused by the misappropriation of the trade secret," and "damages for any unjust enrichment caused by the mis-appropriation."\textsuperscript{41}

The term "trade secret" under the DTSA is defined as:

means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if--

(A) the owner thereof has taken reasonable measures to keep such 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 disclosure or use of the information."\textsuperscript{42}


\textsuperscript{40} Id.


\textsuperscript{42} Id.
While there are some differences between the DTSA and the Uniform Trade Secrets Act, parties often agree that substantively the Uniform Trade Secrets Act and DTSA are "essentially the same," and that courts may look to the state Uniform Trade Secrets Act when interpreting the DTSA. For example, in Kuryakin Holdings, LLC v. Ciro, LLC, a motorcycle aftermarket parts design company filed suit against a competing business, which was started by the company’s departing president, his son, and three of the company’s designers. The company alleged that the defendants misappropriated trade secrets in violation of the DTSA and Wisconsin Uniform Trade Secrets Act. The court first analyzed the claim under Wisconsin’s Uniform Trade Secrets Act, and then applied that same analysis to resolve the DTSA claim. The parties agreed that the DTSA and Wisconsin Uniform Trade Secrets Act were substantively similar and that the court could rely on the Wisconsin Uniform Trade Secrets Act to decide the DTSA claim.

III. CONFIDENTIAL INFORMATION PROTECTION: 3 SCHOOLS OF THOUGHT

Trade secrets have protection under statutory and common law. In franchise cases, the question arises whether the franchisor’s claimed confidential and proprietary information is either a trade secret or otherwise entitled to protection. This section addresses the three schools of thought on whether confidential information under a contract is subject to protection from misappropriation, either as a trade secret or otherwise. Although many of the cases cited in this section are employment cases, the rationale and discussion “for the three schools of thought is more robust than is often found in cases involving whether a franchisor’s claimed confidential information is protectable. As a result, these exemplar cases are instructive for franchise practitioners who deal with confidential information and trade secrets in franchise systems.

A. Confidential Information Protectable Only If It Is A Trade Secret

Massachusetts courts have been most active in holding that confidential information is protected from disclosure only if it is a trade secret. The case law suggests that trade secrets and confidential business information “are essentially identical concepts.” A confidentiality

43 For example, in some states, the Uniform Trade Secrets Act has a provision stating that it does not apply to misappropriations that occur prior to its effective date whereas DTSA does not contain such a provision. Thus, courts have held that the DTSA applies to misappropriations that began prior to the DTSA’s enactment if the misappropriation continues to occur after the enactment date. See Syntel Sterling Best Shores Mauritius Ltd. v. Trizetto Grp., Inc., No. 15–cv–211, 2016 WL 5338550, at *6 (S.D.N.Y. Sept. 23, 2016) (finding viable a continuing misappropriation claim that began pre-enactment because the DTSA defines misappropriation as the "disclosure or use of a trade secret" and the complaint alleged that the defendants "continue[d] to use" the trade secrets after the DTSA was enacted) (emphasis in original) (quoting 18 U.S.C. § 1839(5)(B)); Adams Arms, LLC v. Unified Weapon Sys., Inc., 2016 WL 5391394, at *5–7 (same).


45 Id.

46 Id.

agreement "cannot make secret that which is not secret, and it remains for the court to
determine whether an alleged trade secret is in fact such."48

In United Rug Auctioneers, Inc. v. Arsalen, United sought injunctive relief to prohibit the
defendants from disclosing United’s proprietary and confidential information regarding its
business of selling oriental and Persian rugs. United conducted liquidation sales of oriental and
Persian rugs by auction throughout Massachusetts. It purchased rugs from three vendors in
New York City and the location from which to sell the rugs was of primary importance. United
had historically chosen the locations for the sales in cities and towns that had a high per capita
income because the rugs were handmade and relatively expensive. United would then
advertise the sale by direct mail flyers to households within nearby zip codes. Arie Arsalen, a
friend of United’s owners worked for United from March 2002 to October 2002, and became
intimately acquainted with the details and profitability of United’s business. For each sale,
United retained a file of information that included directions to the site, vendor license
requirements, contact persons, and summaries of prior sales. This file was stored securely by
United and accompanied the United salesperson to the sale location, and was promptly
returned to United upon completion of the sale.

United considered this method of doing business as confidential and required all non-
family employees to sign confidentiality and nondisclosure agreements. Arsalen executed a
confidentiality and nondisclosure agreement in June 2002. Paragraph one of Arsalen’s
Agreement dated June 19, 2002, provides as follows:

1. Nondisclosure of Company's Confidential Information

In the course of Employee's employment with the Company and
because of the nature of Employee's duties and responsibilities,
Employee will acquire knowledge of the Company's confidential
and proprietary information not previously known to Employee and
not known to the general public. Such confidential and proprietary
information includes, but is not limited to, the following: business
and financial information, marketing strategies, lists of the
Company's customers and prospective customers and lists of the
Company's vendors and other sources of supply, all hereafter
referred to as "Proprietary Information." Employee will also acquire
information respecting Proprietary Information which is generally
known to the public, but whose use by the Company or its
affiliates is not generally known and which, if the same was known
to the Employee prior to employment with the Company, is
hereafter also called "Proprietary Information." Employee agrees
that Employee will not, while in the employ of the Company or at
anytime thereafter, directly or indirectly, communicate, divulge,
disclose or make known, or use for the benefit of Employee or of
any other person, firm, association or corporation, any Proprietary

48 Lanier Prof'l Servs., Inc. v. Ricci, 192 F. 3rd 1, 5 (1st Cir. 1999) (quoting Dynamic Research Corp. v. Analytic

Information, whether or not such information is produced by Employee’s own efforts, without the prior written permission of the Company, except that Employee may disclose such matters to the extent disclosure is required (a) in the course of Employee’s employment with the Company to further the interests of the Company or (b) by a court or governmental agency of competent jurisdiction. 50

In the fall of 2002, Arsalen left to open a competing business. In particular, Arsalen met with United’s primary rug supplier and requested the same “mix” of rugs as previously sold to United at the same price; scheduled several rug sales at locations and facilities used previously by United; utilized the same method of advertising, namely direct mail to the adjoining zip codes; advised the advertising agency to make his flyers look exactly like United’s direct mail flyers and solicited several United employees to leave and join his new competitive venture. 51

The Massachusetts court immediately turned its attention to the application of trade secret law concluding that “trade secrets and confidential information are essentially identical concepts.” 52 The court found that United’s vendors, places of sale, times of sale, prices, mix of rugs, and financial information was confidential information deserving of protection from disclosure. In particular, the court noted United’s care in keeping this information secret. “Internally, ... [United] treated this information as confidential and proprietary, took reasonable steps to keep it secure, and did not share it with anyone other than those necessary employees. They kept important files in secure locations. They entered into Confidentiality and Non-Compete agreements with key employees.” 53 The court also found that the sale locations, though seemingly non-confidential, actually were confidential because of the profitability of the locations, which was determined by United by trial and error. 54 Finally, the court found that though the content of the flyers was not confidential, United’s method of promotion was confidential, particularly the zip codes selected and the quantity of flyers sent. 55

Interestingly, the court concluded that:

The evidence in this case is overwhelming that the defendants were doing nothing more than precisely copying United’s modus operandi, and that they operated the business utilizing the information furnished to them by Arsalen in violation of his Agreement. ... It is more than a mere coincidence that [Arsalen’s new company] 1) went to [United’s primary rug supplier] to buy rugs in the same “mix” and for the same price as United; 2) chose

50 Id. at *5.
51 Id. at *1-4.
52 Id. at *6.
53 Id.
54 Id.
55 Id.
locations (towns and facilities) used by United to conduct its sales; and 3) and used the same promotional system used by United, and asked one advertising agency to practically duplicate United’s flyer. That the defendants attempted to hire three of United’s employees is further significant evidence that the information held by United was what [Arsalen’s new company] was after.56

Here, the Massachusetts court enforced the terms of the confidentiality and nondisclosure agreement but did so because it found that the information pilfered by defendants was, in fact, trade secrets. Importantly, United treated this information as a trade secret, protecting the availability of the information to certain individuals, ensuring that those with access to the information were restricted from disclosing the information, and requiring that the information be carefully maintained and returned to its secure storage place immediately upon completion of its use.57 In short, United treated this information as a trade secret, and the court protected it like a trade secret under the trade secret analysis.

In contrast, in Take It Away, Inc. v. The Home Depot, Inc.58 a waste removal services company brought a state court action against Home Depot alleging violation of a non-disclosure agreement, misappropriation of trade secrets, and other claims in connection with its contemplated dumpster supplier business. Home Depot signed a confidentiality and non-disclosure agreement with Take It Away sometime after 1997, when Home Depot received a “teaser” from Take It Away describing Take It Away’s “confidential” business plan.59 Take It Away’s plan was to supply customers of building material supply dealers like Home Depot with dumpsters. Take It Away spent years trying to convince Home Depot to adopt its business plan as Home Depot’s own and use Take It Away to supply the dumpsters and waste removal services. Under the plan, Take It Away would supply Home Depot with dumpsters and Home Depot would rent directly to its customers. Home Depot would retain 10% of the rental value for itself and pay Take It Away the remainder.60 Home Depot was consistently not interested in becoming a dumpster lessor and communicated that to Take It Away over the course of a 5-year pitch by Take It Away.

In 2003, Home Depot signed agreements with four suppliers of waste disposal services to use space in Home Depot stores to offer dumpster rentals directly to Home Depot customers and pay Home Depot a fee for using the Home Depot store floor space.61 Take It Away brought suit alleging that Home Depot violated the non-disclosure agreement by entering into agreements with other suppliers on terms different from Take It Away’s proposal.

56 Id.
57 Id.
58 374 F. App’x 47 (1st Cir. 2010).
59 The First Circuit does not make it clear precisely when Home Depot signed the “non-disclosure agreement,” but presumably after receipt of the “teaser” in 1997.
60 Id. at 48.
61 Id.
The First Circuit identified the key issue in the case: what was actually protectable confidential information?

The principal difficulty in this case is understanding what the confidentiality agreement was supposed to protect. "Confidential Proprietary Information" is undefined, and the district court not unnaturally took it at a fairly general level to cover "the concept of renting dumpsters from national home improvement retail centers." At first, some of us also thought that was what the fight was about, but a careful rereading of Take It Away's reply brief shows that its claim is a degree more particular, focused on brokerage. It says that its "dumpster-brokerage concept and business plan" were the intended subjects of protection; "the essence of its concept is national retail distribution dumpster brokerage" combined with a "separate business plan for putting its concept into practice" (emphasis in original). The stress in the reply brief is repeatedly on its "dumpster-brokerage concept" or "container-brokerage concept," which is more specific than "rental of dumpsters."62

The First Circuit took little time in concluding that there was not enough value in the concept of "brokering" waste suppliers beyond what was commonly known or obvious to amount to consideration for Home Depot's promise to limit its disclosure of such information.63 First, the Home Depot official who signed the Confidentiality and Non-disclosure agreement had already seen a "teaser" that disclosed the business concept to Home Depot without protection.64 As a result, the "brokerage" concept was out in the open before Home Depot agreed to discuss the proposal. Second, even if the claimed secret had not been disclosed before the agreement, the First Circuit found nothing "of value not readily imaginable that might be protected."65 The Court also noted that Home Depot already rented tools and trucks to customers, and that dumpsters were commonly rented out to construction and home improvement businesses. Based on these facts, the Court held that:

it is hard to see what concept or plan Home Depot gained from the disclosure that it could not have thought up readily for itself if it had found any reason to expand its rental activity: a dumpster is a big tool for removing debris, and renting tools and establishing reliable supply networks are not the stuff of novel concepts.66

62 Id. at 48-49.
63 Id. at 49.
64 Id.
65 Id.
66 Id. at 50.
The First Circuit concluded that Take It Away had no protectable trade secret because, among other things, Take It Away did not protect its information, disclosing it in the "teaser."\(^{67}\) In addition, Take It Away's information could have been independently acquired by Home Depot.\(^{68}\) Indeed, virtually every element of the six elements considered in determining if the information is a trade secret cut against Take It Away, including the amount of time and money devoted to the development of the trade secret (here, virtually nothing other than unsuccessful marketing efforts) and the value of the trade secret (here, valuable only through the affiliation with Home Depot, not the value of the purported trade secret).\(^{69}\)

What is most notable is that the First Circuit relied on trade secret analysis in determining whether there was confidential information to protect pursuant to a Confidentiality and Nondisclosure Agreement. This analysis suggests that, at least in Massachusetts, confidential information and trade secrets are interchangeable and the information is protected from disclosure only if it meets the standards of being a trade secret.

Another example is *Agero, Inc. v. Rubin*.\(^ {70}\) Agero provided automobile services to the insurance and automotive manufacturing industries, mostly related to emergency towing and roadside assistance. The defendants were former employees of Agero and signed a confidentiality and non-solicitation agreement when they first began working for the company and again upon their departure from the company. After the defendants left Agero, their new company provided similar but more expensive products to insurance companies. Agero alleged that the defendants misappropriated its trade secrets.

The court relied on *Home Depot* and used the words "confidential information" and "trade secrets" interchangeably. Although Agero alleged misappropriation of trade secrets, the court held that the information taken by the defendants was not confidential information. There was no evidence that the information had substantial value to Agero, nor that the information was a source of revenue for Agero. Further, the allegedly confidential information was not a "carefully guarded secret."\(^ {71}\) Instead, it was advertised in a towing industry magazine and appeared on the company's website and other marketing materials. Finally, the court reasoned that the confidential information was not entitled to protection because the idea itself, "mainly tow truck drivers taking photographs and making them available to view on a website for a price, would be easy to observe and duplicate once the service was available for purchase."\(^ {72}\)

Other courts have taken the same approach as the Massachusetts courts and used the terms "trade secrets" and "confidential information" interchangeably. For example, in *Ram Tool*

\(^{67}\) *Id.*

\(^{68}\) *Id.*

\(^{69}\) *Id.* at 51.


\(^{71}\) *Id.* at 6.

\(^{72}\) *Id.* (citing *Take It Away, Inc. v. The Home Depot, Inc.*, 374 F. App'x 47 (1st Cir. 2010)).
& Supply Co. v. HD Supply Construction Supply Ltd.,73 Ram Tool and HD Supply Construction Supply d/b/a White Cap Construction Supply ("White Cap") were competitors in the construction tools and material distribution industry. The dispute arose because a White Cap employee and recruiter approached Ram Tool employees about working for White Cap. Ram Tool's Nashville branch manager ultimately left Ram Tool in order to work for White Cap and then recruited his sales staff from Ram Tool to join him at White Cap.

Although the Tennessee Court of Appeals opinion was largely focused on other issues, it did address in dicta the trial court's explanation of Tennessee law on trade secrets and confidential information. The court stated that Ram Tool elected to abandon its Tennessee Uniform Trade Secrets Act ("TUTSA") claim, even though the information that formed the basis for the claim would qualify for protection under TUSTA, if proven. The confidential information that the Court found compelling included schedules calculating sales commissions, lists of customers who were called by individuals who left Ram Tool for employment at White Cap, and the number of sales made by those individuals. However, the court explained that Ram Tool's claims depended on "proof that trade secret, proprietary, and/or confidential information – all of which are synonymous under Tennessee case law – was acquired, disclosed, and/or used by the defendants."74 It therefore appears that Tennessee law also recognizes "trade secrets" and "confidential information" as synonymous.

In Missouri, in Brown v. Rollet Brothers,75 a former employee brought a declaratory judgment action against his former employer seeking a declaration that the noncompete and confidentiality agreement he signed were unenforceable. The employee was a dispatcher who had regular contact with customers and prospective customers and would regularly quote the former employer's rates to prospective customers for hauling their commodities. The trial court concluded that the confidentiality agreement was unenforceable. On appeal, Rollet argued that it had a protectable interest in its confidential information, specifically, its customer list, rate sheets, and pricing process. The court concluded that the information sought to be protected by Rollet could be protected only if the information rose to the level of a trade secret.76

In California, it is widely recognized that Section 16600 of the California Business and Professions Code prohibits the enforceability of non-competes.77 However, an exception to Section 16600 is recognized when a non-compete clause is necessary to protect a party's trade secrets. In Scott v. Snelling and Snelling, Inc.78 Scott entered into franchise agreements with


74 Id. at *2.

75 291 S.W. 3d 776 (Mo. Ct. App. 2009).

76 Id. (customer lists are protectable as trade secrets only when they represent "a selective accumulation of information based on past selling experience, or when considerable time and effort have gone into compiling it"); id. at 779 ("[b]y its very nature, defendants' rate sheet was not a trade secret" and "pricing process can be a trade secret").

77 Cal. Bus. & Prof. Code § 16600 ("Except as provided in this chapter, every contract by which anyone is restrained from engaging in a lawful profession, trade, or business of any kind is to that extent void.").

Snelling to operate temporary personnel service (TPS) agencies. Following difficulties between the parties, Scott informed Snelling of its intention to terminate the franchise agreements immediately and form competing TPS businesses at the same locations used for the Snelling franchise locations. In order to overcome the application of Section 16600, Snelling sought to demonstrate the existence and use of trade secrets by Scott. Snelling claimed that, pursuant to the terms of the definition of confidential information in the franchise agreement, its trade secrets included business forms, temporary employee lists, and customer lists. The court granted Scott’s motion for summary judgment because Snelling did not produce evidence that the customer lists constituted a trade secret. They were "easily discoverable through public sources" while Scott had developed its customer lists "through their own efforts, personal knowledge and business contacts." Thus, although California courts prevent unfair competition by a former franchisee taking and using the franchisor’s trade secrets, the misappropriated information must in fact be a trade secret.

In *Flip Flop Shops Franchise Company, LLC v. Neb,* a franchisor terminated a franchisee following a notice of default regarding the franchisee’s failure to pay royalty and brand fund fees. The franchisee, Neb, changed the names of the stores, but continued to operate those stores, selling the same products, using the same displays and the same “System” that was in place in the stores when they were authorized Flip Flop Shops. In applying Delaware law and analyzing the facts in relation to the enforceability of the covenant not to compete, the court made factual findings about the franchisor’s confidential information and its value to the system as a trade secret. The characteristics that distinguished the stores were developed through “a significant amount of effort, research, and resources,” including manuals, operating procedures, market concepts, interior and exterior design, specifications for equipment and supplies, products, management programs, and other standards and specifications. The court found that Flip Flop Shops treated this information as confidential and/or proprietary. Neb admitted that (1) Neb operated these stores in the same location as

---

79 Id. at 1036.

80 Id. at 1037.

81 Id. at 1043.

82 Id.

83 Id.

84 Id. at 1044.


86 Id. at *4.

87 Id.

88 Id. at *2 (The court used the terms confidential information, proprietary information, and trade secrets interchangeably).

89 Id. at *2.

90 Id.
the franchised locations (essentially Flip Flop Shops with changed signage); (2) Neb did not remove but continued to use Flip Flop Shops' commissioned cork flooring, signature cash wraps, and back lit wall displays with tailored "speed rails"; and (3) Neb made only "superficial modifications" to the stores in response to the litigation.91 Since Neb continued to use Flip Flop Shops' confidential information in the former franchised locations, the court concluded that Flip Flop Shops met the standards for issuance of a preliminary injunction to enforce the non-compete and stop the unfair competition.

B. Confidential Information Is Protectable And Is Different From Trade Secrets

The second school of thought is that confidential information is protectable separate and apart from trade secrets. In states that adopt this rationale, courts find confidential information protectable even though the information does not rise to the level of a trade secret. Generally, the information claimed to be protected does not have an independent economic value, an element required in the trade secret analysis.

For example, in Orthofix, Inc. v. Hunter,92 the Sixth Circuit distinguished between trade secrets and confidential information under Texas law. The Court recognized three categories of business information: (1) "trade secrets," (2) contractually protected "confidential information," and (3) "general skills and knowledge."93 In Orthofix, an employee signed a non-disclosure agreement that prevented him from using or disclosing "confidential information," which was defined to include customer lists and identification, business and trade practices, sales or distribution methods and techniques, business strategies, and other information relating to Orthofix's business and financial affairs.94 The employee left Orthofix for employment with a competitor and immediately started selling his old customers the same medical device made by his new employer. After leaving Orthofix, he kept confidential information on his personal laptop and in his memory, which he disclosed to his new employer. The employee argued that the information was not entitled to protection because it "must have a substantial element of secrecy," suggesting that the information must be a trade secret, not merely confidential information subject to a nondisclosure provision.95

The court rejected the employee's argument. It analyzed the relationship between three categories of business information listed above (trade secrets; contractually protected confidential information; and general skills and knowledge). The court concluded that the employee breached the employment agreement by using and disclosing "confidential information," which did not qualify as trade secrets but was more than general skills or knowledge.96 The confidential information not only included the tangible documents, but also

---

91 Id. at *7.
92 630 F. App'x. 566 (6th Cir. 2015).
93 Id. at 567.
94 Id. at 571-72.
95 Id. at 572.
96 Id. at 567.
included information the employee retained in his memory. 97 It reversed the lower court’s holding, which limited protection to trade secrets. Although the court acknowledged a difference between confidential information and trade secrets, the court held that both are entitled to protection. With regard to the confidential information, the court reasoned “while trade-secret status may be denied, the confidence cannot be.” 98

Similarly, in Simplified Telesys, Inc. v. Live Oak Telecom, LLC, 99 a software developer sued former employees and their corporation for misappropriation of trade secrets and confidential information. By research and development, Simplified developed a computer program that initiated the detailed instructions necessary to operate any of three switches used in accounting for certain prepaid telephone cards. 100 The defendants worked on separate steps (10 in all) necessary to develop the program, though Simplified separated the knowledge base of each step to one of the defendants and never aggregated all of the information from the entire 10 steps in one employee (though aggregately, the defendants had worked on 9 of the 10 steps). 101 As a condition of employment, Simplified required the defendants to execute an agreement not to use any “confidential information of the company.” 102 The defendants ultimately left Simplified, aggregated the information they each retained, and developed a computer program to compete with Simplified. The Texas Court of Appeals held that the confidential information obtained by the defendants may be contractually protected, even though it may not be a trade secret. 103 As the court stated:

The confidentiality covenant includes more than “trade secrets.” It embraces any “proprietary information, technical data,” and “know-how, including but not limited to” the designated items. The supreme court has stated that injunctive relief awarded in cases such as this is intended to protect more than the secrecy of information; such relief is also intended to protect against violence to the confidential relationship and the covenants governing the acquisition of confidential information. “Whether the plaintiffs have any valuable secret or not[,] the defendant knows the facts, whatever they are, through a special confidence that he accepted”; and while trade-secret status may be denied, “the confidence cannot be.” 104

97 Id. at 572.
98 Id. at 571 (citing Simplified Telesys, Inc. v. Live Oak Telecom, LLC, 68 S.W.3d 688, 693 (Tex. App. 2000)).
100 Id. at 690.
101 Id.
102 Id.
103 Id. at 693-94.
104 Id. at 692-93 (quoting Hyde Corp. v. Huffines, 158 Tex. 566, 314 S.W.2d 763, 770 (1958)).
The Third Circuit has also held that there is a difference between trade secrets and confidential information and that each is entitled to protection. In Thomas & Betts Corp v. Richards Manufacturing Co., an employer sued a former employee and his new employer alleging that the former employee misappropriated information concerning the design, manufacture, and marketing of a line of underground electrical connector products and used that information to compete against his former employer. The employee had executed a confidentiality and nondisclosure agreement and a covenant not to compete. Richards told the employee that it would not hire him unless his former employer released him from his future employment restrictions. The plaintiff employer, Thomas & Betts agreed to release the employee from his future employment restrictions, but cautioned the employee that "[n]otwithstanding [the release], it is understood that you are not permitted to share or release information proprietary to Thomas & Betts—Elastimold."

The district court dismissed the plaintiff's misappropriation of confidential information claim. The Third Circuit remanded the case to the district court because it found that the district court applied the wrong analysis to the confidential information. Instead of analyzing whether the information was confidential and wrongfully disclosed, the district court went a step further and applied the post-employment noncompetition covenant analysis in assessing whether the nondisclosure obligation was reasonable with respect to duration and geographic scope. That analysis, according to the Third Circuit, is "not relevant in this case, where, whether expressed contractually or not, [employee] had a common law obligation to maintain the secrecy of his employer's proprietary information."

The Third Circuit explained the district court's inquiry on remand:

On remand, the District Court should consider whether the allegedly misappropriated information was provided to [employee] by T & B in the course of his employment for the sole purpose of furthering T & B's business interests. To answer that question, the Court should consider the following factors: (1) whether the information was generally available to the public; (2) whether [employee] would have been aware of the information if not for his employment with T & B; (3) whether the information gave [employee]—and, by extension, Richards—a competitive advantage vis-à-vis T & B; and (4) whether [employee] knew that T & B had an interest in protecting the information to preserve its own competitive advantage. This inquiry does not entail a "rigorous examination of the information sought to be protected," as in trade secret law, but rather a focus on the relationship between employer and employee, the expectations of the parties,
and the intended use of the information. Moreover, it appears to
us that, unlike in trade secret law, these four factors are not to be
treated as essential elements of a cause of action for the
misappropriation of confidential information. 109

In another example, Metro Foods, Inc., v. Kelsch, 110 a former employer sued a former
employee alleging that the former employee used confidential and proprietary information on
behalf of Metro Food’s competitors. The employer’s confidential information included customer
lists, pricing lists, past customer invoices demonstrating purchasing habits, and client specific
manufacturing codes. 111 The employee handbook prohibited employees from disclosing
confidential information acquired during the course of employment to unauthorized persons,
including subsequent employers.

The court recognized that confidential information and trade secrets are different, but
both are entitled to protection. The court relied on the Thomas & Betts factors identified above
to determine whether confidential information would be protected. 112 Further, the court also
followed the Thomas & Betts decision in stating that, unlike trade secret law, it is not necessary
to treat the factors as essential elements of the misappropriation of confidential information
claim. 113 To determine whether there was misuse of information, the court analyzed the
“relationship between the parties at the time of disclosure and the intended use of the
information.” 114 The court noted that, even without an agreement, confidential and proprietary
information is protected, although it does not rise to the level of trade secret status. 115

The Seventh Circuit also concluded that, under Illinois law, confidential information
may be protected, even though it does not rise to the level of a trade secret. In Tax Track Systems
Corp. v. New Investor World, Inc., 116 Tax Track and New Investor World (“NIW”) teamed up to
sell “leveraged life insurance,” life insurance for the very wealthy who need policies of such
great value that the premiums are unusually high. The premium payments are financed with a
loan on which the insured pays only interest and the balance of the loan is paid out with the life
insurance death benefit. 117 Although leveraged life insurance is not a new idea (or proprietary to

109 Id. at 759-60 (citations omitted). Further, with regard to the element that the information is generally available to
1995), a New Jersey court held that customer names were protectable as confidential information, despite the fact
that they were “publicly available” in trade directories, because “the fact that they are customers of [the plaintiff]” was
not publicly available. Id. at 285, 770 A.2d 1158 (quoting Lamorte Burns & Co. v. Walters, 167 N.J. 285, 259-300, 770
A.2d 1158 (2001)).


111 Id. at *1.

112 Id. at *3.

113 Id.

114 Id. at *3 (citing Lamorte Burns & Co v. Walters, 167 N.J. 285, 300, 770 A.2d 1158 (2001)).

115 Id. at *3.

116 478 F. 3d 783 (7th Cir. 2007).

117 Id. at 784.
Tax Track), NIW executed a Confidentiality, Intellectual Property and Non-Disclosure Agreement that bound NIW for a term of three years to keep confidential all “Licensed Material,” including confidential information.\textsuperscript{118} The relationship between Tax Track and NIW terminated after a very short time and NIW began selling a product similar to Tax Track’s leveraged life insurance product using an explanatory memo to clients that “bears striking resemblance” to work product of Tax Track.\textsuperscript{119}

In analyzing whether NIW was liable to Tax Track, the Seventh Circuit concluded that Tax Track “need not show its information rises to the level of a trade secret, but it must nevertheless establish that it engaged in reasonable steps to keep the information confidential.”\textsuperscript{120} Unfortunately, Tax Track failed to establish that it maintained the secrecy of the information.

In the state of Nevada, courts have concluded that confidential information may be protected without regard to whether it is a trade secret. In Saini v. Int’l Game Tech.,\textsuperscript{121} Saini executed a confidentiality agreement while an employee of International Game Technology (“IGT”). IGT sought a preliminary injunction to prohibit Saini’s continued disclosure of IGT’s confidential information and/or trade secrets in violation of the confidentiality agreement. The district court issued a preliminary injunction to prevent Saini from violating the “spirit” of the confidentiality agreement, “regardless of whether the documents reflected confidential information or trade secrets.”\textsuperscript{122} Specifically, the district court found that Saini’s testimony as an expert witness against IGT in separate litigation would amount to improper disclosure of IGT’s confidential information.\textsuperscript{123} The court concluded that while some of the information disclosed by Saini may not be confidential, much of it may qualify as confidential or as a trade secret, which would support a finding that Saini likely breached his agreement.\textsuperscript{124}

C. There Is A Difference Between Confidential Information And Trade Secrets And Only Trade Secrets Are Afforded Protection.

The third school of thought is that there is a difference between confidential information and trade secrets and that only trade secrets are afforded protection. A trade secret is by definition confidential information. However, as discussed above, some courts view trade secrets as subsets of confidential information that are subject to specific protection, but that contractual provisions prohibiting disclosure of “confidential information” are enforceable to protect that information. Other states and courts view provisions prohibiting disclosure or use of confidential information much like covenants not to compete and scrutinize them to determine

\textsuperscript{118} Id. at 785.

\textsuperscript{119} Id. at 786.

\textsuperscript{120} Id. at 787 (citing Tower Oil & Tech. Co. v. Buckley, 99 Ill. App. 3d 637, 425 N.E.2d 1060, 1066 (Ill. Ct. App. 1981)).

\textsuperscript{121} 434 F. Supp. 2d 913 (D. Nev. 2006).

\textsuperscript{122} Id. at 924.

\textsuperscript{123} Id. at 918-19.

\textsuperscript{124} Id. at 924.
whether they are necessary to protect a legitimate interest and are reasonable with respect to duration and geographic scope.

One example of a case where the court found that confidential and trade secret information were not synonymous and protected only the trade secret information is Calisi v. Unified Financial Services, LLC. The plaintiff, Calisi, worked as an accountant for United Financial Services ("UFS"). After his employment ended, he began working for Messina who emailed over 2,000 clients, some of whom were also clients of UFS. The lower court found that Calisi misappropriated UFS’s customer lists and personal information. However, the Arizona Court of Appeals disagreed.

UFS argued that it took steps to keep the client information confidential, including using confidentiality clauses in employment agreements, upgrading its electronic security system, terminating former employees’ access rights, and compiling financial regulations regarding protection of clients’ personal information. However, the court concluded that the confidential information was not entitled to protection because it was not a trade secret. The court recognized “although there may be substantial overlap between confidential information and trade secrets, they are not synonymous.” Therefore, the court reversed the lower court and entered judgment in Calisi’s favor, holding that the confidential information was not entitled to protection because it was not a trade secret.

In Georgia, protection of confidential information has been the subject matter of court cases, legislation, and constitutional amendment. In 1993, the Georgia Supreme Court differentiated between confidential information and trade secrets when it held that a customer list in "tangible" form might be protected as a trade secret, but a customer list in "intangible" form "in the minds of former employees" was not protectable as a trade secret. The Georgia legislature responded by amending the Georgia Trade Secrets Act to extend protection to information without regard to form.

Prior to amendments to the Georgia Trade Secrets Act, Georgia law prohibited unlimited protection of confidential information. In Pregler v. C&Z, Inc., the Georgia Court of Appeals considered whether a confidentiality and nondisclosure agreement between an employer and employee was enforceable where it contained no time limit for the protection of the confidential information. The court held that "a nondisclosure clause with no time limit is unenforceable as to information that is not a trade secret." The court relied on Georgia’s Constitution, which

---

126 Id. at 109.
127 Id.
128 Id.
130 Ga. CODE ANN. § 10-1-761(4).
131 575 S.E. 2d 915, 917 (Ga. 2003).
132 Id.
provided that “all contracts and agreements which may have the effect, or be intended to have the effect, to defeat or lessen competition, or to encourage monopoly, shall be illegal and void.” 133 In 2010, the voters of Georgia approved an amendment to their Constitution to “make Georgia more economically competitive by authorizing legislation to uphold reasonable competitive agreements.” 134 The new Georgia legislation not only specifically applies to franchisors and franchisees,135 but also explicitly states:

nothing in this article shall be construed to limit the period of time for which a party may agree to maintain information as confidential or as a trade secret, or to limit the geographic area within which such information must be kept confidential or as a trade secret, for so long as the information or material remains confidential or a trade secret, as applicable.136

Wisconsin, on the other hand, takes a different view. In Tatge v. Chambers & Owen,137 the employee, Tatge, entered into a confidentiality and nondisclosure agreement and covenant not to compete. The Court concluded that the enforceability of the confidentiality and nondisclosure agreement was governed by Wisconsin statute Sec. 103.465, which states:

A covenant by an assistant, servant or agent not to compete with his or her employer or principal during the term of the employment or agency, or after the termination of that employment or agency, within a specified territory and during a specified time is lawful and enforceable only if the restrictions imposed are reasonably necessary for the protection of the employer or principal. Any covenant, described in this section, imposing an unreasonable restraint is illegal, void and unenforceable even as to any part of the covenant or performance that would be a reasonable restraint.138

Despite the statute’s specific reference to covenants not to compete, the court, relying on Gary Van Zeeland Talent, Inc. v. Sandas,139 concluded that a nondisclosure agreement without temporal restrictions was a clear attempt by the employer to restrain competition.

133 GA. CONST. ART III, § 6(V)(c)(2).
134 See GA 2010 Constitutional Amendment Ballot proposal. It is worth noting, however, that contracts entered into before November 3, 2010 are interpreted and analyzed pursuant to the former interpretive framework established by common law.
135 GA. CODE ANN. § 13-8-52(a)(5).
136 GA. CODE ANN. § 13-8-53(e).
137 219 Wis.2d 99, 579 N.W. 2d 217 (Wis. 1998).
138 WIS. CODE ANN. § 103.465.
139 84 Wis.2d 202, 267 N.W. 2d 242 (Wis. 1978).
"[I]t is clear that Chambers & Owen seeks to restrain competition through use of the non-disclosure provision. It seeks to shield its customer data, programs, and business practices from competitors' eyes because it "represents an asset of substantial value." This is the essence of a trade restraint; it would be an exercise in semantics to overlook Wis. Stat. § 103.465 merely because paragraph 1 of the agreement is not labeled a "covenant not to compete."\(^{140}\)

In Wisconsin, therefore, confidential information may only be protected for a reasonable amount of time, even though the confidential information may have value of longer duration. As a result, Wisconsin courts will scrutinize whether a nondisclosure provision is reasonable rather than simply enforcing the provision to protect confidential information.\(^{141}\)

IV. PRACTICE POINTERS

Considering the principals discussed above, there are some practical steps a party seeking to protect information from disclosure should undertake. First, it is incumbent upon franchise practitioners and franchisors to analyze the franchise system carefully to determine what information is truly proprietary or commercially sensitive and should be maintained as confidential. For example, customer contacts may be a protectable commodity, because goodwill develops between customers and the business due to the business representatives' contact with those customers.\(^{142}\) On the other hand, a "customer list" that is essentially a list of the names and phone numbers that discloses only publicly available information, is likely not protectable.\(^{143}\) Keeping in mind the standards set forth in the cases cited above, great care should be given to each and every part of the system to determine what specifically should be categorized as confidential information.

Once that information is identified, steps must be taken to properly limit the disclosure of such confidential information. For example, in Tax Track Systems Corp. v. New Investor World, Inc.,\(^{144}\) a case discussed above, the Seventh Circuit suggested that the only "conceivable" information that could have been confidential in that case was the work product of Tax Track that was essentially copied by NIW.\(^{145}\) The Court turned to its analysis in Rockwell Graphic Systems, Inc. v. DEV Industries., Inc.\(^{146}\)

\(^{140}\) Chambers & Owen, 579 N.W. 2d at 222.

\(^{141}\) See Techworks, LLC v. Willie, 770 N.W.2d 727 (Wis. 1998) (holding that a two year noncompete limitation is within the ambit of reasonableness); H&R Block Eastern Enters., Inc. v. Swenson, 745 N.W.2d 421 (Wis. Ct. App. 2007) (holding that two-year duration of restrictive covenant was reasonable, but extension of the two-year period would be unreasonable); Pollack v. Calmag, 458 N.W. 2d 591 (Wis. Ct. App. 1990) (holding that two-year restraints generally are considered reasonable in Wisconsin).

\(^{142}\) Brown v. Rollet Bros., 291 S.W. 3d at 777.

\(^{143}\) Id. at 776.

\(^{144}\) 478 F.3d 783 (7th Cir. 2007).

\(^{145}\) Id. at 787.

\(^{146}\) 925 F.2d 174, 180 (7th Cir.1991).
"Rockwell Graphic Systems, a trade secrets case, involved "piece part" drawings, which were detailed drawings of parts for Rockwell machines that indicated materials used, dimensions, tolerances, and methods of manufacture. Rockwell stamped the drawings "Confidential" and kept them in a vault with limited access. The drawings could be used by Rockwell's 200 engineers, who had to sign them out and replace them after use. All photocopies had to be destroyed. Rockwell also gave some third-party manufacturers copies of the drawings because it sometimes hired them to build the parts. Everyone who had access to a drawing signed a confidentiality agreement. Noting that disclosure of confidential information is often necessary to profit off the information, we held in Rockwell Graphic Systems that the mere fact the drawings were shared with third-party manufacturers did not necessarily destroy the confidential nature of the documents as a matter of law."147

The Court held that Tax Track had not treated its work product as confidential under the Rockwell Graphics Systems analysis. The work product was distributed to 600-700 people and no more than 190 of them signed confidentiality agreements. This widespread non-confidential disclosure was fatal to Tax Track's claims that this information should be protected as confidential information under Illinois law.148

The Tax Track case also illustrates the challenge that franchise systems face when trying to protect information that the franchisor subjectively "believes" is confidential. A typical franchisor may believe that the entire contents of its operations manual and most elements of its system are confidential. However, franchisors likely disclose this purportedly confidential information to "600 – 700 people" in disseminating the manual to franchisees (who may in turn give employees access to the manual). Moreover, aspects of the system (restaurant layout, for example) become publicly disclosed simply through operation of the business.

Since some states will not protect confidential information that does not rise to the level of a trade secret, should a franchisor classify every part of its system as a trade secret in order to have protection in all states? The challenge with that approach is that, as noted above, large parts of a franchisor's system that the franchisor might believe are confidential will not meet all of the elements of a trade secret. For example, some information sought to be classified as a trade secret most likely will not have independent economic value outside of the system as a whole.

An illustration of this risk is Little Caesar Enterprises, Inc. v. Sioux Falls Pizza Company, Inc.149 In that case, the franchisee operated Little Caesars franchises in Sioux Falls until expiration of the franchise agreements. Immediately upon the expiration of the franchise agreements, the former franchisee opened a competing pizza restaurant at the location of one

147 Tax Track Sys. Corp., 478 F. 3d at 788 (citations omitted).

148 Id.

of the former Little Caesars franchised locations, and continued to offer “all day, every day ready-for-pick-up” pizza.\textsuperscript{150} Little Caesars alleged that the former franchisee misappropriated trade secrets. Specifically, Little Caesars argued that its system for preparing and selling ready-for-pick-up whole pizzas in a competitive fashion was a trade secret that should be protected.\textsuperscript{151} The Court discussed alleged trade secrets:

Little Caesars has come forward with minimal proof that its system in producing Hot-N-Ready pizza could be the type of information that is a method, technique, process, or program under a broad view of the definition of trade secret. The most specific information given to the court by Little Caesars about the system is that its "calculations specify how many pepperoni pizzas, cheese pizzas, crazy bread and chicken wings the franchisee should prepare and when each component of the preparation process should occur." The system also includes that the pizza dough is specially prepared, specially stored, and allowed to rise for a specific period of time. Then the sauce and toppings have to be applied in a special way and cooked for a specific amount of time. Finally, the finished product must be stored in accordance with the specifics of the system. Little Caesars also stated during oral argument that it believed the trade secret is the process of profitably or successfully selling an all day, every day ready-for-pick-up pizza at a low price point. Later when pressed, Little Caesars argued that the protectable trade secret also included the "projection" or "build-to" charts and other internal proprietary documents within the system that helped franchisees determine their expected flow of traffic and otherwise predict business patterns.\textsuperscript{152}

The court then analyzed whether Little Caesars' purported trade secrets had independent economic value:

Little Caesars did not make a clear showing of, and the court could not discern, specifically which information within Little Caesars' system is "not generally known." General references to preparation, timing, and amounts of food per hour to minimize waste is not specific enough to constitute a trade secret and would not classify as being "not generally known." Little Caesars has brought forth evidence that its system has economic value because its business is successful and it claims to have a substantial market share of the carryout pizza industry. Little Caesars has not distinguished, however, how that system has brought them specific economic value above and beyond the

\textsuperscript{150} Id. at *1.

\textsuperscript{151} Id. at *3.

\textsuperscript{152} Id. at *5 (citations omitted).
generic knowledge of how to run a restaurant that provides ready-made pizza.

***

The evidence presented in the hearing demonstrated that Pizza Patrol proofed or sheeted out its dough, let it rise in the pan, spread on sauce, cheese, and toppings, baked the pizza, and put it under a heat lamp in preparation for sale. ... [T]here was evidence that many proprietors of pizza restaurants prepare their dough in the same manner. At this stage in the litigation, Little Caesars only presented evidence that its system is a general or common sense way of preparing and making pizza or that defendants were doing nothing more than what every other pizza proprietor in the restaurant business accomplishes.\textsuperscript{153}

The Court next analyzed whether Little Caesars took appropriate steps to maintain the secrecy of its purported trade secrets.

Little Caesars took some steps to safeguard its proprietary information by forcing all franchisees to sign confidentiality agreements about the system and Little Caesars' business practices, but that confidentiality did not extend to all employees with direct exposure to the system. ... Although the franchisees were those charged with upholding the Little Caesars brand and implementing any terms of the franchise agreement, it was the employees of Little Caesars who actually prepared and completed each step in the system. Those employees prepared the dough, applied toppings, baked the product, sold it to customers, and determined when product was no longer fresh enough to keep. Thus, those with the most detailed knowledge of Little Caesars' system were people who had no duty or promise to keep that information confidential because they were not required to sign confidentiality agreements and did not have access to the "confidentially" marked operations guide.\textsuperscript{154}

The Court concluded that at the preliminary injunction stage of the litigation, Little Caesars did not demonstrate that it took reasonable efforts to maintain the secrecy of its purported trade secrets.

\textit{Little Caesar Enterprises, Inc. v. Sioux Falls Pizza Company, Inc.} is demonstrative of the risk that a franchisor runs by attempting to classify its entire system as a trade secret.\textsuperscript{155} Franchisors need to carefully analyze all parts of their system, separately classify trade secrets from other confidential information and protect the information accordingly. If the information is

\textsuperscript{153} Id. at *5 -6 (citations omitted).

\textsuperscript{154} Id. at *7 (citations omitted).

\textsuperscript{155} This case involved the same franchisee who created the "Hot-N-Ready" pizza concept for Little Caesars and was involved in litigation over the trademark "Hot-N-Ready" with Little Caesars. \textit{See Pinnacle Pizza Co. v. Little Caesar Enterprises, Inc.}, 396 F. Supp. 2d 891, 896 (D.S.D. 2005) (describing the original Hot-N-Ready concept).
truly a trade secret (such as a proprietary recipe or a confidential list of customers contacts), then the franchisor must be meticulous in taking appropriate measures to protect the trade secret from widespread disclosure. This becomes more difficult in a franchise system where trade secrets are disclosed to franchisees and franchisee employees, because the potential for unintentional disclosure by those parties that could undermine a claim for trade secret protection.

Should a franchisor avoid the challenges to trade secret protection and simply classify proprietary information as confidential? In some jurisdictions, as described above, confidential information will be protectable even if it does not rise to the level of a trade secret. However, in some jurisdictions, there is no protection afforded to confidential information that is not itself a trade secret. The best advice is to separate trade secrets from confidential information, and then establish safeguards for the protection of each. As discussed earlier, the protection of trade secrets and confidential information requires that the efforts to maintain secrecy be “reasonable under the circumstances.” Courts do not require that extreme and expensive procedures be taken to protect trade secrets. Although there is no precise definition of what is a reasonable effort to maintain the secrecy of a trade secret, the following steps, albeit not an exhaustive list, have been held to be reasonable efforts to maintain secrecy: (1) controlled disclosure to employees and licensees; (2) limiting access to confidential information to individuals with a need to know; (3) limiting access to confidential information in computer systems to those with passwords; and (4) requiring execution of carefully drafted confidentiality agreements that are not overbroad and are tailored to the system’s protectable information.

Attached as Appendix 1 are sample provisions defining “confidential information” from various franchise industries, such as restaurant, home health care, and urgent care systems. What is plain from the provisions is that no one provision or definition will work for all systems. Careful consideration must be given to the needs of the system and the information potentially at issue when drafting provisions in franchise agreements defining “confidential information.”

Franchise practitioners must also give consideration to confidentiality concerns in non-disclosure and confidentiality agreements (“NDAs”) used in the franchise relationship. For example, if a franchisor discloses confidential information or trade secrets during the sales process and before a franchise agreement is signed, it is critical that the franchisor first obtain executed NDAs signed by any parties to whom such information will be disclosed. Franchisors must comply with the disclosure requirements and waiting periods in the applicable state before a prospect can sign the NDA. In addition, franchisors must obtain executed NDAs from all parties to whom confidential information and trade secrets will be disclosed, such as all owners of a business entity franchisee and all franchisee representatives and managers who attend training sessions. Finally, as indicated in Little Caesar Enterprises, Inc. v. Sioux Falls Pizza Company, Inc.,156 franchisors may want to consider requiring franchisee employees “with the most detailed knowledge” of the franchisor’s system who “have direct exposure to the system” to sign NDAs related to franchisor’s confidential information and trade secrets.157

Likewise, franchise practitioners should give consideration to confidentiality issues when drafting settlement agreements. For example, consider a scenario where a franchisee subject to

---


157 Id. at *7.
post-termination obligations reaches an agreement (prior to litigation or arbitration) on terms to exit the system, but continue to operate a similar business at the same location. Whatever the terms of the settlement are, the franchisor will likely want to make sure those terms are kept confidential by the former franchisee to prevent those terms from being disclosed to other franchisees. Presumably the particular terms of the settlement will be unique to that particular franchisee and its business situation. Regardless, the franchisor may not want other franchisees to know those terms and attempt to negotiate a similar arrangement even though the circumstances are different. Franchisors should also consider including agreed language that both parties will use to explain the resolution without revealing the terms (e.g., "The parties reached a confidential agreement under which Franchisee ceased operating a franchised business and secured the right to continue operating independently."). A franchisor would also want language prohibiting the former franchisee from using the franchisor’s trade secrets and confidential information in the new business, and require return of any such information in the possession of the former franchisee. Even though the franchisee would likely have those obligations under post-termination provisions of the franchise agreement, reiterating those requirements in the settlement agreement ensures that there is no confusion or argument that the settlement agreement supplants the franchise agreement on these issues. Franchisors should also be aware that the existence of confidentiality provisions in their settlement agreements may need to be disclosed in Item 20 of their Franchise Disclosure Document.

The same issues would arise in settling litigation or arbitration. Again, the franchisor will likely want to make sure that the settlement agreement and its terms are kept confidential by the former franchisee for the reasons discussed above. However, in the case of a favorable settlement, particularly one in which the litigation is being watched by other franchisees in the system, the franchisor may wish to dispense with the confidentiality requirement and publicize the settlement to its franchisees as a means of setting an example. These agreements should also prohibit the former franchisee from using the franchisor’s trade secret and confidential systems and information and require the return of any such information in the possession of the former franchisee. In addition to considering the implications on Item 20 of the franchise disclosure document, franchisors will also want to consider the implications of confidential settlement agreements on their obligations to disclose settled litigation matters in Item 3 of the franchise disclosure document. If the confidentiality obligations are mutual, the franchisor will need to ensure that it has the right to disclose the terms of the settlement as required by law, including for Item 3 disclosure purposes, for tax and audit purposes, and as may otherwise be required by a court of law.

V. LITIGATING CONFIDENTIALITY CLAUSES IN FRANCHISE AGREEMENTS

When a franchisor must file a lawsuit to protect its trade secret or confidential information, the franchisor must be in a position to prove that the information is a trade secret or confidential information. That requires a franchisor to identify with particularity the trade secret(s) or confidential information that warrants protection. At the same time, a franchisor must remember to be realistic about the information it seeks to protect. Seeking to protect too much information may anger the decision-maker and put “real” trade secrets or confidential information at risk. Also, franchisors must be sure not to disclose the confidential information in the public record or open court; the information must be disclosed pursuant to protective order
or under seal. Otherwise, the secrecy of the information may be lost in the process of litigating its protection.\textsuperscript{158}

To prove the information is a trade secret or confidential information, the franchisor must present evidence that the information is secret, is not known to others, is not publicly available and is subject to confidentiality provisions in the franchise agreement.\textsuperscript{159} Franchise systems as a whole may be sufficient to show confidential/trade secret information even where individual components of the system would not suffice.\textsuperscript{160} However, the franchisor must prove that despite the fact that the entire franchise system may have access to the information, the franchisor has ensured that the information is maintained in confidence by its franchisees by establishing how the franchisor limited access to that information.\textsuperscript{161}

For example, in Snelling & Snelling, Inc. v. Armel, Inc.,\textsuperscript{162} the franchisor signed a franchise agreement with the defendant for the operation of an employment agency business using the Snelling & Snelling system. The parties agreed that the methods and techniques employed by Snelling & Snelling were of considerable value and that the operations manuals and information contained therein were confidential, not to be disclosed outside the Snelling system, or used by defendants in competition with Snelling & Snelling.\textsuperscript{163} Further, Snelling & Snelling, through the substantial expenditure of time, effort and money, and as a result of the studies and surveys made by it over numerous years, had compiled and developed procedures, techniques, methods of operations, training manuals and instructional guides relating to employment office management and the hiring, training and supervision of employees, and certain forms and other methods, all of which were designed to give the system a competitive advantage over other employment agencies.\textsuperscript{164} All of the aforesaid were kept confidential by Snelling & Snelling and its franchisees and were not disseminated and not available to others.\textsuperscript{165} In light of the foregoing, the court found that the Defendants improperly operated competitive employment agencies in violation of the franchise agreement and used the information,

\textsuperscript{158} Gov't Employees Ins. Co. v. Nealey, 262 F. Supp. 3d 153, 168 (E.D. Pa. 2017) (reasonable measures to protect the secrecy of the plaintiffs alleged trade secrets were not taken where confidential information was disclosed in affidavit).

\textsuperscript{159} See Sections IIA through IID, supra.; see also Mark S. VanderBroek and Christian B. Turner, Protecting and Enforcing Franchise Trade Secrets, 25 Franchise L.J. 191, 196-97 (Spring 2006) (discussing evidence necessary to prove each element of a trade secret claim when a franchisor brings a claim for misappropriation of trade secret information).

\textsuperscript{160} See Cici Enters., L.P. v. Four Word Motion, LLC, 2016 WL 924466, at *9 (where former franchisee was operating restaurant using former franchise system's proprietary information to operate nearly identical pizza restaurant, court found violation of Florida Trade Secrets Act).

\textsuperscript{161} Id. at *11 (Franchisees were required to sign franchise agreement, which contained thorough confidentiality agreement barring franchisees and controlling principals from using confidential information).

\textsuperscript{162} 360 F. Supp. 1319 (W.D. La. 1973).

\textsuperscript{163} Id. at 1320.

\textsuperscript{164} Id.

\textsuperscript{165} Id.
techniques, methods of operation and procedures disclosed in confidence to them by Snelling & Snelling.\textsuperscript{166}

Likewise, in \textit{The Quizno's Corp. v. Kampendahl},\textsuperscript{167} Quizno's brought an action against a former franchisee claiming he breached the franchise agreement when he subsequently opened a sandwich shop, Bob's Deli, at the same location after termination. Bob's Deli closely resembled Quizno's in its menu and in the content of its sandwiches.\textsuperscript{168} In some cases, the sandwiches at Bob's Deli followed the same recipe and only the names had changed.\textsuperscript{169} In other cases, the recipes and names were identical.\textsuperscript{170} Bob's Deli also used the same equipment.\textsuperscript{171}

The court in Quizno's pointed out that the former franchisee "acknowledged in the [franchise agreement] that anything revealed to him by Quizno's-including the Operations Manual as well as Quizno's system in its entirety-constituted trade secrets."\textsuperscript{172} The former franchisee argued that he was not misappropriating any trade secret, because information that is known generally through observation is not a secret and making a sandwich is too simple to constitute a trade secret.\textsuperscript{173} The court, however, determined that the franchisee's definition of "secret' was too narrow.\textsuperscript{174} This was so, because the former franchisee was not just making sandwiches; rather, the former franchisee was using recipes, menus, signs and ovens initially approved as part of a Quizno's business strategy.\textsuperscript{175} Additionally, the court noted that the franchisee acknowledged in the franchise agreement that the Quizno's system constituted a trade secret.\textsuperscript{176}

However, if the information is not kept confidential or only kept confidential in part, courts will be inclined to find that non-confidential disclosure is fatal to claims that the information should be protected.\textsuperscript{177} For example, in \textit{Stockade Cos., LLC v. Kelly Restaurant Group, LLC},\textsuperscript{178}

\begin{footnotes}
\textsuperscript{166} Id.
\textsuperscript{167} No. 01C6433, 2002 WL 1012997 (May 20, 2002).
\textsuperscript{168} Id. at *2.
\textsuperscript{169} Id.
\textsuperscript{170} Id.
\textsuperscript{171} Id.
\textsuperscript{172} Id. at *6.
\textsuperscript{173} Id.
\textsuperscript{174} Id.
\textsuperscript{175} Id.
\textsuperscript{176} Id.
\textsuperscript{177} \textit{Tax Track Systems Corp.}, 478 F.3d at 787.
\end{footnotes}
a buffet-style franchise system brought a misappropriation of trade secret claim under the Texas Uniform Trade Secrets Act against a former franchisee that was operating a competing restaurant at the former franchise location. The franchise system argued that the “buffet system” constituted “protectable trade secrets under Texas law.”\textsuperscript{179} However, “buffet system” was defined by the franchisor and in the franchise agreement broadly.\textsuperscript{180} One of the franchisor’s employees testified that the franchisor defined the system as “the recipes, the manuals, the training materials, our staff...all of our vice president[s], directors that help operate the franchises and develop systems and process[es] to help us operate our restaurants.”\textsuperscript{181} He further stated that the “buffet system” is “everything.”\textsuperscript{182} The court determined that, even if the “indeterminate laundry list elements comprises a ‘trade secret,’” the former franchisee did not acquire the information through a breach of a confidential relationship or discover it by otherwise improper means such that it would be able to make out a claim for misappropriation of trade secrets. The Court noted that (i) the former franchisee was not using the franchisor’s “buffet system” in its entirety; (ii) there was evidence that the franchisor disposed of allegedly secret information, including recipes, in a public, unlocked dumpster; and (iii) the employees of the franchisee were not required to sign confidentiality agreements and the former employees could have put their knowledge to use for a competitor.\textsuperscript{183}

Likewise, with regard to misappropriation of customer and member lists, practitioners should focus on presenting evidence of the specific compilation of the lists and not arguing the system generally is confidential. For example, in American Express Financial Advisors v. Yantis,\textsuperscript{184} American Express alleged that it had protectable confidential information in (a) its client names, addresses, and data, including suitability information, investments and investment history, financial plans, and financial goal information; (b) prospective client names, addresses, and data; and (c) know-how concerning the methods of operation, client lists and other financial information.\textsuperscript{185} In applying the Iowa Trade Secret Act, the court found that American Express had shown that the information fell within the definition of “trade secret” as the information was a compilation of information about American Express’s clients and their financial histories.\textsuperscript{186} The court also found that the information would derive economic value from not being generally known to and not being readily ascertainable by proper means by a person able to obtain economic value from its disclosure or use as the information would be helpful to American Express’s competitors and would require cost, time and effort to duplicate.\textsuperscript{187} American Express also presented evidence that it protected the secrecy of the information by requiring financial

\textsuperscript{179} Id.
\textsuperscript{180} Id.
\textsuperscript{181} Id.
\textsuperscript{182} Id.
\textsuperscript{183} Id. at *5 and n.4.
\textsuperscript{184} 358 F. Supp. 2d (N.D. Iowa 2005).
\textsuperscript{186} Id. at 831.
\textsuperscript{186} Id.
\textsuperscript{187} Id. at 832.
advisors to sign confidentiality agreements and financial advisors agreed to have staff having access to this information sign confidentiality agreements.\textsuperscript{186}

In contrast, in \textit{BJM & Associates, Inc. v. Norrell Servs., Inc.},\textsuperscript{189} the franchisor of a temporary employment agency attempted to prove that the general “know-how” of its system provided to franchisees was unique.\textsuperscript{190} However, no proof was submitted at trial evidencing that the system was unique. Rather, the evidence showed that the franchisor’s customer lists, business forms and procedures, and temporary employee list were not trade secrets, because they were readily discoverable through public sources.\textsuperscript{191} The franchisee also proved at trial that it had developed its own customer list, without any assistance from the franchisor.\textsuperscript{192} More specifically, the franchisor failed to prove that it had provided the franchisee a business lead or contact for a client.\textsuperscript{193} Further, as to the methods and procedures comprising the system, the franchisee showed that the franchisor’s forms and procedures are in general use in the industry and that they could be purchased over the counter from private vendors.\textsuperscript{194} Accordingly, the court found that the “methods, business forms, and procedures that comprise the [franchisor’s system] are not trade secrets.”\textsuperscript{195}

Equally important, a franchisor must prove the value of the trade secret, such as the amount it cost to develop the system and the confidential information. In \textit{Gold Messenger, Inc. v. McGuay},\textsuperscript{196} the court discussed that while the precise value of the operations manual was in dispute, there was evidence that the information contained in the manual did have some value. Specifically, the court found that the manual “did provide an advantage over other competitors,” and the court held that the while in the hands of the defendant, the confidential information produced several issues of a competing publication, which generated revenue.\textsuperscript{197} Similarly, confidential lists of names of potential franchisees in the Re/Max system and confidential reports showing the sales produced by top sales associates in the Re/Max system and their commissions, which were compiled over a period of time by an individual hired to assist Re/Max in the sale of franchises, reflected a substantial investment of time and money by Re/Max.\textsuperscript{198}

\textsuperscript{186} \textit{Id.}

\textsuperscript{189} 855 F. Supp. 1481 (E.D. Ky. 1994).

\textsuperscript{190} \textit{Id.} at 1496.

\textsuperscript{191} \textit{Id.} at 1497.

\textsuperscript{192} \textit{Id.}

\textsuperscript{193} \textit{Id.}

\textsuperscript{194} \textit{Id.}

\textsuperscript{195} \textit{Id.}

\textsuperscript{196} 937 P.2d 907 (Colo. App. 1997).

\textsuperscript{197} \textit{Id.} at 911.

\textsuperscript{198} \textit{See Re/Max of Am., Inc. v. Viehweg}, 619 F. Supp. 621, 626 (E.D. Mo. 1985) (ordering former employee of Re/Max to return to Re/Max documents containing confidential information, which constituted trade secrets).
Trade secret protection may also exist even where no agreement exists. In *Tan-Line Studios, Inc. v. Paul*, the franchisor hired the defendant to assist with the sale of franchises. Instead, the defendant teamed with others to develop a competing tanning company based on the information they obtained from Tan-Line. In determining whether the defendant was liable for theft of trade secrets, the court applied the Restatement of Torts § 757 and analyzed whether the information appropriated was a trade secret. The court found that a trade secret indeed existed, because the individuals on behalf of Tan-Line developed a particular method of doing business that is peculiar to Tan-Line and is not known in the industry and includes Tan-Line’s business methods. The court further found that one of the best pieces of evidence supporting Tan-Line’s argument that the entire business methodology constitutes a trade secret is that franchisees are willing to purchase a franchise.

Another important aspect of the *Tan-Line* decision is the import the court placed on the novelty of the information with respect to the defendant’s effort to develop a competitive business. The court found that just because the defendant might have been able to duplicate the plaintiff’s business methods through investment of his own did not preclude trade secret protection. Instead, the court held that the defendant could not steal the information from Tan-Line, regardless of whether it might have duplicated it legitimately through other means. In fact, the court noted that there was no evidence to show that the defendant obtained the information independently and without misappropriating it from Tan-Line. Because Tan-Line protected its trade secrets by not sharing the information with anyone other than managing shareholders and the information was not known outside the company, the court had no issue deciding that the franchisor had maintained the confidentiality of the information.

What is evident from these cases is that there is no clear path to protect trade secrets and confidential information in a franchise system, particularly because each state has its own laws defining trade secrets. Thus, while it is necessary to identify and confirm the definition of “trade secret” in the appropriate jurisdiction, protecting such information must begin long before litigation arises. This protection should include drafting confidentiality provisions after thoughtful consideration with franchise counsel, and ensuring the provision defines the trade secrets and confidential information and requires the franchisee to acknowledge that the confidential information has financial value. Additionally, the franchisor should implement appropriate steps to maintain the secrecy of its trade secrets and confidential information. Such steps include requiring franchisees and controlling principals to sign confidentiality provisions; protecting critical, competitive sensitive information using reasonable security to maintain confidentiality; limiting access to the confidential information only to those to whom it is necessary; and

---


200 *Id.* at *7.*

201 *Id.*

202 *Id.*

203 *Id.*

204 *Id.* at *9.*
requiring return of trade secret and confidential information upon termination or expiration of the franchise agreement.

VI. CONCLUSION

It is evident that protecting trade secrets and confidential information varies from state to state and under federal law. Much like the varying laws to which franchisors are subject with respect to covenants not to compete and franchise disclosure and relationship laws, there is no single correct way to ensure that a franchisor will be able to protect its trade secrets and confidential information. However, franchisors may be better able to protect their trade secret and confidential information if they keep in mind the legal framework and practices discussed above and adopt procedures to keep their information confidential. Such processes may be necessary for the ultimate protection of the information that distinguishes the system from a competitor brand and that provide the value for which franchisees pay to enter the system.
APPENDIX 1

Definition of Confidential Information

In Home Care Facility

CONFIDENTIAL INFORMATION
The following Sections of the Franchise Agreement shall define the term "Confidential Information" for purposes of this Agreement:

11.3 Confidential Information
During the term of this Agreement and following the expiration or termination of this Agreement Franchisee covenants not to communicate directly or indirectly, nor to divulge to or use for its benefit or the benefit of any other person or legal entity, any trade secrets which are proprietary to Franchisor or any information, knowledge or know-how identified to Franchisee by Franchisor in writing as confidential (including but not limited to the Operations Manual) or otherwise deemed confidential under Sections 7.2 and 11.2 of this Agreement, except as permitted by Franchisor. In the event of any expiration, termination or non-renewal of this Agreement, Franchisee agrees that it will never use Franchisor’s Confidential Information, trade secrets, methods of operation or any proprietary components of the ______ Program in the design, development or operation of any business providing (a) supplemental healthcare staff to institutional clients, such as hospitals, nursing homes and clinics, and/or (b) comprehensive care, including medical and non-medical services, to private duty clients within their home or residence. Notwithstanding the foregoing, the obligations in this Section 11.3 shall not apply to information: (a) which at the time of disclosure is readily available to the trade or public; (b) which after disclosure becomes readily available to the trade or public, other than through breach of this Agreement; (c) which is subsequently lawfully and in good faith obtained by Franchisee from an independent third party without breach of this Agreement; (d) which was in possession of such party prior to the date of disclosure; or (e) which is disclosed to others in accordance with the terms of a prior written authorization between the parties to this Agreement. The protections granted hereunder shall be in addition to and not in lieu of all other protections for such trade secrets and confidential information as may otherwise be afforded in law or in equity.

Definition of Confidential Information

Urgent Care Facility

CONFIDENTIAL INFORMATION

(1) We possess (and will continue to develop and acquire) certain Confidential Information, some of which constitutes trade secrets under applicable law, relating to developing and operating Franchised Businesses and Centers, including:

(a) site selection and territorial criteria;
(b) training and operations materials and manuals;
(c) methods, formats, specifications, standards, systems, procedures, sales and marketing techniques, knowledge, and experience used in developing and managing Centers and providing urgent care and accessible primary care services to patients;
(d) marketing and advertising programs for Centers;
(e) physician and employee recruitment, training, and retention programs;
(f) knowledge of, specifications for, and suppliers of Operating Assets, and other products and services;
(g) any computer software or similar technology which is proprietary to us or the System, including, without limitation, digital passwords and identifications and any source code of, and data, reports, and other printed materials generated by, the software or similar technology;
(h) knowledge of the operating results and financial performance of Centers and Franchised Businesses (subject to compliance with HIPAA and other requirements); and
(i) graphic designs and related intellectual property.

(2) You acknowledge and agree that you acquire no interest in the Confidential Information by virtue of this Agreement or otherwise, other than the right to use it as we specify in operating the Franchised Business during this Agreement’s term, and that the Confidential Information is proprietary and is disclosed to you only on the condition that you agree that you:

(a) will not use Confidential Information in any other business or capacity;
(b) will keep each item deemed to be part of Confidential Information absolutely confidential, both during this Agreement’s term and then thereafter for as long as the item is not generally known in the employment and/or health care and/or urgent care industries;
(c) will not make unauthorized copies of any Confidential Information disclosed via electronic medium or in written or other tangible form; and
(d) will adopt and implement reasonable procedures to prevent unauthorized use or disclosure of Confidential Information, including restricting its disclosure to Franchised Business personnel and others and using non-disclosure and non-competition agreements with those having access to Confidential Information. We have the right to regulate the form of agreements that you use and to be a third-party beneficiary of those agreements with independent enforcement rights. You are obligated to maintain in your files, those executed confidentiality agreements we specify and make them available to us upon request.

(3) Confidential Information does not include information, knowledge, or know-how which you can demonstrate lawfully came to your attention before we provided it to you directly or indirectly; which, at the time we disclosed it to you, already had lawfully become generally known in the health care management and/or urgent care industries through publication or communication by others (without violating an obligation to us); or which, after we disclose it to you, lawfully becomes generally known in the health care management and/or urgent care industries through publication or communication by others (without violating an obligation to us).

Definition of Confidential Information

Daycare Facility

Confidentially Agreement

Confidential Information means information, or a compilation of information, in any form (tangible or intangible), related to the System and any other aspects of your or the Franchisor's business that the Franchisor has not made public or authorized public disclosure of and that is not already generally known to the public or to other persons who might obtain value or competitive advantage from its disclosure or use. The Franchisor's Confidential Information includes, but is not limited to: the Manual (the "Manual") and its contents, and other business
methods; business plans and analysis; marketing plans and strategies; information regarding franchisees and prospective franchisees; research and development data; trade secrets; copyrightable materials; knowledge, know-how, methods and techniques; computer programs; innovations and un-patented inventions; and information about third parties (including, but not limited to, customers and franchisees) that such third parties provide to you or the Franchisor in confidence (such as financial or personal information, student lists, and student information).
Mark J. Burzych

Mark Burzych is a founding member of Fahey Schultz Burzych Rhodes, PLC in Okemos, Michigan, and leads the firm’s business practice. His practice focuses on business expansion and development with an emphasis on legal issues related to franchising, trademark registration and enforcement, licensing and regulation (with a focus on liquor licensing), corporate issues, business and finance transactions, real estate, and other business-related matters. Mark’s business practice is one of a very limited full-service franchise practices in the state of Michigan. It is specially tailored to the franchise industry, but his experience allows him to assist virtually any business industry or segment.

In his 25 years of franchise law experience, Mark has represented clients in the food service, restaurant, furniture, hotel, home service, automotive service, child care, child services, and dry cleaning industries as counsel to the franchisors. His niche is representing emerging brands to assist them with designing and implementing their growth strategies, which many times includes franchising. In addition, Mark often represents national brands as local counsel in Michigan, colleagues in the Forum as local counsel in Michigan litigation, or as Michigan counsel in Michigan regulatory matters, such as liquor licensing.


Mark is an active member of the American Bar Association Forum on Franchising, and the International Franchise Association.
Nina Greene

Nina Greene is a partner in the Miami office of Genovese, Joblove & Battista, P.A., where she practices in the areas of franchise, trademark and complex commercial litigation. She has represented franchisors throughout the United States in matters involving protection of trademarks, franchise terminations, discrimination claims, covenants not to compete, unfair competition, business torts and many other issues. She has lectured on numerous franchise issues for the ABA Forum on Franchising and the International Franchise Association (“IFA”). Additionally, Greene is the co-chairperson for the South Florida Chapter of the Women’s Franchise Network of the IFA and is a member of the IFA Supplier Forum Advisory Board. Greene has been selected to appear in Best Lawyers of America, the “International Who’s Who of Business Lawyers” and the “International Who’s Who of Franchise Lawyers.” She is also a committed volunteer and is the National State Advisory Board Chairperson, who oversees all Advisory Boards throughout the United States for Best Buddies, a non-profit organization dedicated to ending the social, physical and economic isolation of individuals with intellectual and developmental disabilities. Greene earned her LL.M. in taxation from Temple University School of Law, her juris doctor from the University of Miami School of Law and her bachelor of arts from the University of Pennsylvania.