AMERICAN BAR ASSOCIATION
35TH ANNUAL FORUM ON FRANCHISING

PROTECTION OF FRANCHISE SYSTEM TRADE SECRETS AND CONFIDENTIAL INFORMATION, AND ENFORCEMENT OF NON-DISCLOSURE AGREEMENTS, IN THE DIGITAL AGE

Michael J. Lockerby
Foley & Lardner LLP
Washington, D.C.

James P. Mittenthal
Epiq Systems, Inc.
New York, New York

Heather Carson Perkins
Faegre Baker Daniels LLP
Denver, Colorado

October 3 – 5, 2012
Los Angeles, CA

Table of Contents

PROTECTION OF FRANCHISE SYSTEM TRADE SECRETS AND CONFIDENTIAL INFORMATION, AND ENFORCEMENT OF NON-DISCLOSURE AGREEMENTS, IN THE DIGITAL AGE

I. OVERVIEW

Another type of intellectual property—the franchisor's trademark—is widely recognized by the federal courts as the "cornerstone of a franchise system."[1] Although franchising may well be "a sophisticated form of trademark licensing,"[2] most if not all franchisors also license the use of their trade secrets. With respect to trademark protection, the "rules of the road" are clear. Trademarks are protected by a federal statute, the Lanham Act, that expressly preempts inconsistent state laws."[3]

Trade secret protection, in contrast, is a function of state law—much of it judge-made, at least until recently. Although most states have adopted the Uniform Trade Secrets Act, there are some places in which the law of trade secrets is anything but uniform. And while it may be the franchisor's trademark that identifies "a network of stores whose very uniformity and predictability attracts customers,"[4] one or more of the franchisor's trade secrets may account for much of that "uniformity and predictability." Unlike the franchisor's prominent if not famous trademark, the franchisor's trade secrets are by definition hidden—and in some cases unknown. Complicating matters further is that trade secrets may be present in all aspects of the franchised business. Recipes and formulas, for example, are an important component of many restaurant and other franchise systems. Depending upon the facts and circumstances, however, trade secret protection may also extend to many other aspects of the franchise. These include methods of doing business, strategic business plans, customer lists and information, planned promotional campaigns, and computer software, to name a few.

As the Internet has become the preferred method of communication in franchise systems, the challenges for protecting trade secrets have become even more daunting. With the click of a mouse, or one touch of a keypad, secrecy may be compromised—and perhaps lost forever. Recent technological advances make it easier to detect security breaches and to verify the extent of the damage after the fact. Based on this experience, the authors offer recommended "best practices" for protecting trade secrets and confidential information, and enforcing non-disclosure agreements, in the digital age. These best practices include recommendations for internal procedures to ensure that the franchisor's own employees and franchisees are not the source of leaks. Departing employees and franchisees in particular often have an incentive to try to take franchise system trade secrets with them. Exit interviews,

---

[1] *Susser v. Carvel Corp.*, 206 F. Supp. 636, 640 (S.D.N.Y. 1962), *aff'd*, 332 F.2d 505 (2d Cir.), *cert. granted*, 379 U.S. 885 (1964), *cert dismissed*, 381 U.S. 125 (1965).

[2] *Power Test Petroleum Distribs., Inc. v. Calcu Gas, Inc.*, 754 F.2d 91, 97 (2d Cir. 1985).

[3] The Lanham Act is "intended . . . to protect registered marks used in such commerce from interference by State, or territorial legislation . . ." 15 U.S.C. § 1127. "If a conflict arises between federal and state law, including state registration statutes, the Lanham Act effects a limited preemption of state law, resolving the conflict in favor of the federal registrant's rights." *Spartan Food Sys., Inc. v. HFS Corp.*, 813 F.2d 1279, 1284 (4th Cir. 1987). *See also Storer Cable Communications v. City of Montgomery, Ala.*, 806 F. Supp. 1518, 1540 (M.D. Ala. 1992) (Lanham Act preempts state laws that "permit[] an erosion of trademark rights") (*citing Mariniello v. Shell Oil Co.*, 511 F.2d 853, 858 (3d Cir. 1975)).

[4] *Principe v. McDonald's Corp.*, 631 F.2d 303, 309 (4th Cir. 1980).

monitoring, and other forms of "self-help"—including forensic verification—are among the recommended best practices.

Even the best of practices, however, will not necessarily protect the franchise system's trade secrets from misappropriation. This paper therefore concludes with recommendations as to how best to pursue wrongdoers—hopefully before it is too late. In this regard, a preliminary injunction may often be the only effective means of damage control. At the federal and state level alike, "computer crimes" statutes may provide the most effective civil remedies—assuming that electronic means were used to access or disclose the trade secrets at issue. This is especially true because the unauthorized access or disclosure itself may be actionable—regardless of whether trade secret protection (if any) has been lost in the process.

II. TRADE SECRETS AND CONFIDENTIAL INFORMATION: DO YOU KNOW THEM WHEN YOU SEE THEM?

A. The Legal Framework

1. Development of Trade Secret Law

"The essential rights of a trade secret owner are the right to use the trade secret and disclose it to employees and others standing in a confidential or contractual relationship with the owner subject to restrictions on unauthorized use or disclosure."[5]

According to the *Restatement (Third) of Unfair Competition*, the protection of confidential business information dates back to Roman law, which afforded relief against a person who induced another's employee to disclose secrets related to the master's commercial affairs.[6] The modern law of trade secrets evolved in England, apparently as a result of the growing accumulation of technical know-how and the greater mobility of employees as the Industrial Revolution progressed.[7]

The existence and protectability of trade secrets was recognized in the United States in the mid-1800s in *Peabody v. Norfolk*.[8] In that key case, the court held that (1) a secret manufacturing process is property which can be protected against misappropriation; (2) an obligation of secrecy for an employee outlasts the term of employment; (3) a trade secret can be disclosed in confidence to others who need to practice it; and (4) the recipient can be enjoined from unauthorized use.[9]

---

[5] Roger M. Milgrim, *Milgrim on Trade Secrets* § 1.01 at 1-4 ("*Milgrim*").

[6] RESTATEMENT (THIRD) UNFAIR COMPETITION § 39, cmt. a (1993).

[7] *Id.*

[8] *Peabody v. Norfolk*, 98 Mass. 452 (Mass. 1868).

[9] *Id.*

2. What is a "Trade Secret"?

a. The Definitions and Interplay of the *Restatements* and the UTSA

In 1939, the common law of trade secrets as it existed then was codified into Section 757 of the *Restatement of Torts*. The definition and framework laid out in the *Restatement* largely prevailed until the 1980s, when states began adopting the American Law Institute's Uniform Trade Secrets Act ("UTSA").[10] Section 757 of the Restatement of Torts and its comments remain often cited, despite the near-universal adoption of the UTSA. Section 757 sets out the following definition:

> A trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity 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.[11]

Comment b to Section 757 proposed six factors to be considered in assessing whether particular information qualifies as a trade secret:

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

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

(3) the extent of measures taken by the trade secret owner to guard the secrecy of the information;

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

(5) the amount of effort or money expended by the trade secret owner in developing the information;

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

These factors have been cited with approval in virtually every United States jurisdiction.[12] Courts routinely apply these six factors in determining whether information qualifies as a trade

[10] The subject matter of Section 757 was intentionally deleted from the *Restatement (Second) of Torts*, which was released in 1978, and assigned for coverage in the *Restatement of Unfair Competition*, which was released in 1995.

[11] RESTATEMENT OF TORTS § 757 (1939).

[12] *Milgrim* § 1.01[1] n.3 (collecting cases by jurisdiction)

secret, both for purposes of common law trade secret misappropriation and when analyzing claims under various states' versions of the UTSA.[13]

In 1979, the National Conference of Commissioners on Uniform State Laws promulgated the Uniform Trade Secrets Act. In the years following the release of the UTSA, nearly all states and the District of Columbia have adopted the UTSA or some variation thereof. In 1994, the American Law Institute published the *Restatement (Third) of Unfair Competition*. This was intended to apply to actions under the common law and to replace Section 757 of the *Restatement of Torts*. The UTSA "codifies the basic principles of common law trade secret protection."[14] As of this writing, the UTSA has been enacted in one form or another in at least forty-five states and the District of Columbia.[15]

Under the UTSA, a trade secret is:

> information, including formula, pattern, compilation, program, device, method, technique or process that
>
> (i) derives independent economic value 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 reasonable efforts under the circumstances to maintain its secrecy.[16]

The UTSA's definition of a trade secret has been described as both substantive and procedural.[17] Substantively, the UTSA's definition is very similar to the definition in Section 757, except that the UTSA does not require that information be used continuously in one's trade or business to be protected.[18] Procedurally, the UTSA adds a requirement. The trade secret claimant must show that the information in question was the subject of efforts to maintain its secrecy, which were reasonable under the circumstances.[19] Even with the adoption of the UTSA by the majority of states, the *Restatement*'s definition and guidelines continue to have force for courts interpreting and applying the UTSA[20]

---

[13] *See, e.g.*, *Harvey Barnett, Inc. v. Shidler*, 338 F.3d 1125, 1129 (10th Cir. 2003) (quoting provisions of Colorado version of UTSA and engaging in extensive analysis of section 757's definitional factors in determining, for purposes of summary judgment, that a genuine issue of material fact existed with respect to whether the plaintiff had a trade secret). *See also Milgrim* § 1.01[2] n.8 (collecting cases by jurisdiction).

[14] NAT'L CONFERENCE OF COMM'RS ON UNIF. STATE LAWS, UNIFORM TRADE SECRETS ACT, prefatory note (1985) ("UTSA"). *See, e.g., Electro-Craft Corp. v. Controlled Motion, Inc.*, 332 N.W.2d 890, 898 (Minn. 1983) (stating the test under Section 757 is "now more or less embodied" in the Minnesota version of the UTSA.)

[15] The states that have not adopted some version of the UTSA are Massachusetts, New York, North Carolina, and Texas.

[16] UTSA §1(4)

[17] *Milgrim* § 1.01.

[18] *Compare* UTSA §1(4) *and* RESTATEMENT OF TORTS § 757.

[19] UTSA § 1(4)(ii).

[20] *See Milgrim* §1.01[2] at 1-28 to 35 (cataloging courts in states that have adopted UTSA relying on Section

Under *Restatement of Unfair Competition* Section 39, "a trade secret is 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." Section 39 replaces the material originally contained in Section 757 and is intended to apply to both actions under the UTSA and at common law.[21] In view of the widespread adoption of the UTSA when the *Restatement (Third) of Unfair Competition* was published, the *Restatement (Third) of Unfair Competition* has been relied on less by courts than the formulation of the UTSA and Section 757.

b. Application

The two key concepts for determining what information qualifies as a trade secret are its secrecy and whether the information has economic value. To be protected, "information must be secret, and its value must derive from the secrecy. In addition, the owner of the information must use reasonable efforts to safeguard the confidentiality of the information."[22] "An exact definition of a trade secret is not possible."[23] Rather, a claim that information qualifies as a trade secret "must be ascertained through a comparative evaluation of all the relevant factors, including the value, secrecy, and definition of the information and the nature of the defendant's misconduct."[24] As the author of a prominent treatise has observed,

> Some characteristics of a trade secret require proof of negative conditions: the alleged trade secret is not generally known in the trade; the alleged trade secrets has *not* been disclosed in such a manner as to constitute loss of secrecy or abandonment. Proof of affirmative conditions is also required: the trade secret is used; the trade secret affords a competitive advantage.[25]

757's elements to determine whether a trade secret exists).

[21] In addition to the common law and statutory definitions employed in civil cases, there are also criminal statutes that relate to trade secrets. For example, the Economic Espionage Act, 18 U.S.C. §§ 1831-1839 (1996) ("EEA") makes it a felony to sell, disseminate, or otherwise deal in trade secrets, or attempt to do so, without the owner's consent. Under that statute, trade secret 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, the public[.]

[22] *Montgomery County Ass'n of Realtors, Inc. v. Realty Photo Master Corp.*, 878 F. Supp. 804, 814 (D. Md. 1995), *aff'd*, 91 F.3d 132 (4th Cir. 1996).

[23] RESTATEMENT OF TORTS § 757, cmt. b.

[24] RESTATEMENT (THIRD) UNFAIR COMPETITION § 39, cmt. d.

[25] *Milgrim* § 1.09 at 1-508.

i. Secrecy

To be a trade secret, the information must not be generally known to, or readily ascertainable by proper means by, the public or competitors.[26] "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."[27] The secrecy "need not be absolute" but rather must only be "sufficient to confer and actual or potential economic advantage on one who possesses the information."[28]

"Proper means" for ascertaining information include observing it in public use, gleaning information from published literature, independent development or invention of the information, or reverse engineering.[29] The fact that individual pieces of information claimed to be part of a trade secret are available to the general public will not necessarily defeat a trade secret claim, however, if the value of the information "stems from its compilation or collection in a single place or in a particular form which is of value."[30] The UTSA defines "improper means" of obtaining information to include "theft, bribery, misrepresentation, breach or inducement of a breach of duty to maintain secrecy, or espionage through electronic or other means."[31]

Whether information is generally known or readily ascertainable through proper means can be a highly fact-intensive inquiry. There is no requirement of "novelty" or "tangibility" as required by other doctrines of intellectual property law, such as copyright or patent. But, the information cannot be immediately evident. As a general rule, the more time or work required to figure out the relevant information, the more likely it is to be a trade secret.[32] On the other hand, if the information is easily derived from examining the product on sale to the public or from the alleged trade secret owner's public interactions (such as marketing materials or presentations), then the information is less likely to be deemed to be a trade secret.[33]

ii. Independent Economic Value From Not Being Readily Ascertainable

In addition, the information must derive independent economic value from not being readily ascertainable. Value may be established either by direct or circumstantial evidence.[34] Direct evidence can include evidence related to the content of the secret and its impact on the operations of the business.[35] Circumstantial evidence can include the investment the plaintiff

---

[26] *Motor City Bagels, LLC v. The American Bagel Co.*, 50 F. Supp. 2d 460, 479 (D. Md. 1999).

[27] RESTATEMENT (THIRD) UNFAIR COMPETITION, § 39, cmt. f.

[28] *Id*.

[29] UTSA § 1 cmt.

[30] *Mettler-Toledo, Inc. v. Acker*, 908 F. Supp. 240, 247 (M.D. Pa. 1995). *See also Harvey Barnett, Inc.,* 338 F.3d at 1129; *Comprehensive Tech. Intern., Inc. v. Software Artisans, Inc.*, 3 F.3d 730, 736 (4th Cir. 1993).

[31] UTSA § 1 cmt.

[32] *Morlife, Inc. v. Perry*, 56 Cal. App. 4th 1514 (Cal. App. 1st Dist. 1997).

[33] *Sun Media Sys., Inc. v. KDSM, LLC*, 564 F. Supp. 2d 946, 969 (S.D. Iowa 2008) (holding that advertiser's method for laying out advertisements not a trade secret when specific concepts taught by the plaintiff were well known throughout the advertising information).

[34] RESTATEMENT (THIRD) UNFAIR COMPETITION § 39, cmt. e.

[35] *Id.*

has made in developing the trade secret information[36] or the efforts the plaintiff took to maintain confidentiality, on the theory that investment or secrecy establish value.[37] Although not required, actual use of the trade secret in the operation of a business is itself some evidence of value.[38] Generally, value is not disputed, so long as the value is more than trivial.

iii. Reasonable Efforts to Preserve Confidentiality

Finally, one claiming trade secret protection must take reasonable steps to keep the information secret. The steps need only be "reasonable under the circumstances;" "extreme and unduly expensive procedures" need not be taken.[39] This element is often disputed in trade secret cases. Because the standard is based on the particular circumstances, the inquiry is often highly factual unless the proponent made no effort to protect the information.[40] Specific protective measures are discussed in detail below.

c. "Confidential Information" versus "Trade Secrets"

Although the author of a leading trade secret treatise has opined that "[t]erminology may not be so very important,"[41] a number of courts have recognized a difference between trade secrets and confidential information. Whether or not this difference leads to a difference in protection is a question with murky answers—even among a state's own courts. The Massachusetts courts have been particularly active in this area. Currently, there appear to be three schools of thought.

The first is that the terms 'confidential information' and 'trade secret' can be used interchangeably. A federal court applying Massachusetts law took this view in *Take it Away, Inc. v. Home Depot*.[42] There, the court noted that "Massachusetts case law does not always define clearly whether trade secrets are synonymous with confidential information or proprietary information. Nevertheless, the case law does suggest that trade secrets and confidential information are essentially identical concepts." The Massachusetts Court of Appeals came to the same conclusion in *Chomerics, Inc v. Ehrreich*, stating that "in context, the references to 'confidential information,' 'confidential know-how,' and similar expressions to which the trial judge allude[d], are merely conclusions of law that certain matters are protectable."[43]

---

[36] *See, e.g.*, *Hatfield v. AutoNation, Inc.*, 939 So. 2d 155, 157-58 (Fla. Dist. Ct. App. 2006) (focusing on substantial investments made by plaintiff).

[37] *See, e.g., Pinchereira v. Allstate Ins. Co.*, 190 P.3d 322, 334 (N.M. 2006); *see also Curtis 1000, Inc. v. Suess,* 24 F.3d 941, 947 (7th Cir. 1994) (if a party seeking to protect its information "did not think enough of it to expend resources on trying to prevent lawful appropriation of it, this is evidence that it is not an especially valuable interest").

[38] RESTATEMENT (THIRD) UNFAIR COMPETITION § 39, cmt. e.

[39] UTSA § 1 cmt.

[40] *Tax Track Systems Corp. v. New Investor World, Inc.*, 478 F.3d 783, 785 (7th Cir. 2007) (granting summary judgment on trade secret claim where "no reasonable jury could conclude that [plaintiff's] meager and inconsistent protective measures where sufficient to protect its information").

[41] *Milgrim* §1.01[1] n. 1 at 1-6.

[42] *Take it Away, Inc. v. Home Depot, Inc.*, 2009 WL 458552, at *8 (D. Mass. Feb. 6, 2009) (Woodlock, J.).

[43] *Chomerics, Inc. v. Ehrreich*, 12 Mass. App. Ct. 1, 3 (1981).

The second view is that there is a difference between trade secrets and confidential information, but both are entitled to protection. In *Tax Track Systems Corp v. New Investor World*, [44] the court concluded that, for the purposes of a breach of confidentiality agreement claim, the plaintiff was not required to show that "its information rises to the level of a trade secret." The court did, however, require that *Tax Track* "establish that it engaged in reasonable steps to keep [the information] confidential." The opinion suggests that confidential information differs from a trade secret in that it lacks one of the two key concepts that define trade secrets—it need not derive independent economic value from not being generally known.

A federal court applying Nevada law reached a similar conclusion in *Saina v. IGT.* There, the court set out distinct definitions for both trade secret and confidential information. Although the court looked to Nevada law for the definition of a trade secret, it recognized that "there is no definition of 'confidential' information under Nevada law" and so, instead, the court relied on Black's Law Dictionary which "defines 'confidential as entrusted with the confidence of another or within his secret affairs or purposes; intended to be held in confidence or kept secret; done in confidence."[45]

In *Thomas & Betts Corp*., the Third Circuit applying New Jersey law developed a set of factors to determine whether confidential information not rising to the level of a trade secret would be protected.[46] The factors the court considered were whether (1) the information was generally available to the public; (2) the defendants would have been aware of the information but for their employment; (3) the information gave the defendants a competitive advantage over their former employer; and (4) defendants knew that the plaintiff had an interest in protecting the information.[47]

The third school of thought holds that is that there is not only a difference between confidential information and trade secrets, but that only trade secrets will be afforded protection. Given the definition of a trade secret, by virtue of being a trade secret, the information would also classify as confidential information. However, some courts view trade secrets as subsets of confidential information that are subject to particular protection.

In *Brown v. Rollet Bros*., the Missouri Court of Appeals analyzed whether information contained on a trucker's rate sheet was confidential information for purposes of enforcing a covenant not to compete. The court relied on a distinction drawn by the Missouri Supreme Court, where confidential information was found to differ "from other secret information in a business in that it is not simply information as to single or ephemeral events in the conduct of business" whereas "a trade secret is a process or device for continuous use in the operation of the business."[48] Applying that analysis to the rate sheets, the court held that although the

---

[44] *Tax Track Systems Corp.*, 478 F.3d at 787.

[45] *Saina v. IGT*, 434 F. Supp. 2d 913, 924 (D. Nev. 2006). *See also Warner-Lambert Co. v. Execuquest Corp.*, 427 Mass. 46, 48–49 (1998) (recognizing that "confidential and proprietary business information may be entitled to protection, even if such information cannot claim trade secret protection").

[46] *Thomas & Betts Corp. v. Richards Mfg. Co.*, 2009 U.S. App. LEXIS 16837, at *10 (3d Cir. Jul. 30, 2009) ("[u]nder New Jersey law, information that does not rise to the level of a trade secret may nevertheless be entitled to protection and may serve as the basis for a tort action"); *Lamorte Burns & Co. v. Michael Walters,* 770 A.2d 1158, 1167 (N.J. Sup. Ct. 2001).

[47] *Thomas & Betts Corp. v. Richards Mfg. Co.*, 2009 U.S. App. LEXIS 16837, at *10-11.

[48] *Russel Brown v. Rollet Bros. Trucking Co.*, 291 S.W.3d 766, 779 (Mo. App. 2009).

confidential information in the rate sheets "may have been valuable to a competitor when they were issued, they had a relatively short useful life," and declined to enforce the covenant not to compete and confidentiality agreement as to the rate sheets.[49]

Georgia also appears to regard this distinction as dispositive. In Georgia's Trade Secrets Act, customer lists are expressly considered to be trade secrets. However, the Georgia Supreme Court differentiated between confidential information and trade secrets when it held that while a tangible customer list might be subject to trade secret protection, an intangible customer list "maintained in the minds of former employees" was not.[50] The Georgia General Assembly responded by amending Georgia's Trade Secrets Act to extend protection to information without regard to form, yet at least one commentator does not believe the change has any impact on the *Avnet* ruling.[51]

Prior to Georgia's adoption of its Trade Secret Act, Georgia law prohibited perpetual protection of confidential information *Pregler v. C&Z, Inc.* is illustrative. There, the Georgia Court of Appeals evaluated whether or not a particular non-disclosure agreement between an employer and an employee was enforceable where it contained no time limit for 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."[52] The court relied on Georgia's Constitution, which states, "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." The court also rejected the blue-pencil rule which allows courts to "sever that part of the covenant which makes the entire covenant unenforceable."[53] Because the court declined to sever the unenforceable clause, the entire agreement was rendered unenforceable.

In November of 2010, Georgia voters approved to amend the state constitution. A clause was added that allowed the General Assembly to authorize and provide enforcement for contracts that restricted competition amongst certain parties. The amendment also gave explicit permission for the courts to blue-pencil these contracts. Included among these parties were employers and employees, as well as franchisors and franchisees.[54] This paved the way for the Georgia legislature to enact new non-compete statues. The new non-compete statutes specifically apply to franchisors and franchisees, among others,[55] and explicitly state:

> 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

[49] *Id*.

[50] *Avnet, Inc. v. Wyle Laboratories, Inc*, 263 Ga. 615 (1993).

[51] C. Geoffrey Weirich & Daniel Hart, *Protecting Trade Secrets and Confidential Information in Georgia*, 60 MERCER L. REV. 533, 539 (2009).

[52] *Pregler v. C&Z, Inc.*, 259 Ga. App. 149, 152 (2003).

[53] *See Richard Rita Pers. Servs. Int'l Inc v. Kot*., 229 Ga. 314, 315-18 (1972) (Supreme Court of Georgia declining to apply the blue-pencil theory citing three Georgia cases where one unreasonable clause rendered the entire non-disclosure or covenant not to compete unenforceable. The court also stated policy concerns that the blue-pencil rule would lead to employers fashioning overly restrictive agreements, with the expectation that courts would pare them down and enforce them).

[54] GA. CONST. art. III, § 6, (V)(c)(2).

[55] GA. CODE. ANN. § 13-8-52(a)(5).

or as a trade secret, for so long as the information or material remains confidential or a trade secret, as applicable.[56]

On the other end of the spectrum, some courts impose time limits for restrictive covenants that protect information that does not rise to the level of trade secret. In Wisconsin, for example, courts considering non-disclosure agreements look to Wisconsin statute § 103.465. This statute governs non-competes and other restrictive covenants such as nondisclosure agreements and confidentiality clauses. In *Tatge v. Chambers & Owen*, the court held that although § 103.465 explicitly refers to covenants not to compete, the court would also apply the statute to non-disclosure provisions.[57] Under the statute, restrictive covenants are enforceable where the covenant is limited to "a specified territory and during a specified time" and "the restrictions imposed are reasonably necessary for the protection of the employer or principal."[58] This 'reasonable' standard can lead to rather unpredictable outcomes. Wisconsin courts have acknowledged that "whether a restrictive covenant is reasonably necessary to protect the employer depends on the totality of the circumstances and is a question of law to be resolved on the basis of either factual findings made by the circuit court or a stipulation of all the relevant facts by the parties."[59] Despite the uncertainty and fact-specific nature of the 'reasonableness' inquiry, Wisconsin courts have generally approved restrictive covenants limited to about two years.[60]

B. Common Types of Trade Secrets in Franchising

Franchise systems own a variety of types of trade secrets and other confidential information. Indeed, it is not unusual that much of the value of a franchise is contained in the franchise system's trade secrets. Depending on the type of business, such trade secrets can include business systems, methods for providing goods or services, product information, recipes, operational standards and procedures, and customer and prospect information. As the broad definitions of a trade secret discussed above suggest, nearly any information is theoretically protectable as a trade secret. The devil is in the details. Whether a particular item will qualify as a trade secret will depend on the facts of the particular case. We have collected below some representative cases dealing with the types of trade secret information often owned by franchise systems

1. Recipes and Formulas

For some franchise systems, a recipe, product, or formula is a crucial element of the system. Certainly, a product formula or recipe can be protected. The classic example is the formula for Coca-Cola. Although most of the ingredients in Coca-Cola are publicly known, the

---

[56] *Id*. § 13-8-53(e).

[57] *Tatge v. Chambers & Owen*, 219 Wis. 2d 99, 112 (1998).

[58] Wis. Stat. § 103.465 (2011).

[59] *Farm Credit Servs. V. Wysocki*, 237 Wis. 2d 522, 529 (Ct. App. 2000).

[60] *See Techworks, LLC v. Willie*, 770 N.W.2d 727 (Wis. 1998) (a two year non-compete limitation is within the ambit of reasonableness); *H&R Block Eastern Enters., Inc., v. Swenson*, 307 Wis. 2d 390 (Ct. App. 2007) (two-year duration of restrictive covenant was reasonable but extension of the two-year period would be unreasonable); *Pollack v. Calimag*, 157 Wis. 2d 222 (Ct. App. 1990) (two-year restraints generally are considered reasonable in Wisconsin).

ingredient that gives the drink its distinctive taste is a secret combination known only to two people within the company. In addition, a court has found that the company has gone above and beyond the reasonable efforts to protect the formula given that "[t]he only written record of the secret formula is kept in a security vault at the Trust Company Bank in Atlanta, Georgia, which can only be opened upon a resolution from the Company's Board of Directors."[61]

Similarly, Kentucky Fried Chicken's seasoning formula has been held to be a trade secret.[62] The court noted that KFC maintained "unilateral and complete control over KFC seasoning" by using only two suppliers, each of which was given access to only a portion of the recipe as to which the supplier had agreed to maintain the secrecy of the formula.[63]

However, the trade secret protections of recipes and formulas are sometimes challenged. For example, a former Quizno's franchisee contended that Quizno's sandwich recipes were not trade secrets because: (1) the information was "known generally through observation or may be developed through means available to the public;" and (2) "making a sandwich is too simple a notion to constitute a trade secret."[64] The court rejected the argument, finding that the franchisee's construction of the trade secret was too narrow because he was not merely making sandwiches, but was also using recipes, menus, signs, and ovens that were initially approved as part of his franchise. The court noted that the franchisee had also acknowledged in the franchise agreement that the Quizno's system constituted a trade secret.[65]

On the other hand, common recipes, formulas, and information that are publicly available or easy to duplicate may not qualify for trade secret protection.[66] In the *Arthur Treacher's* case, the court held that the franchisor's food preparation process was neither unique nor a secret. The court held that "there [was] no evidence, [other than the testimony], that the temperature at which plaintiff fries food, or the length of time the food is immersed in oil, or the length of time the food is held after frying, is a trade secret of plaintiff's or is even any different from the process used by plaintiff's competitors."[67] The court also noted that the franchisor had failed to take steps to protect the confidentiality of the information, including failing to enforce a confidentiality clause in its agreement, and that "probably thousands" of current and former employees knew about the cooking process. Finally, the court stated that the cooking methods were ascertainable to "anyone with a modicum of intelligence."[68]

---

[61] *Coca-Cola Bottling Co. v. Coca-Cola Co.*, 107 F.R.D. 288, 294 (D. Del. 1985).

[62] *KFC Corp. v. Marion-Kay Company*, 620 F. Supp. 1160, 1172 (S.D. Ind. 1985).

[63] *Id.*

[64] *The Quizno's Corp. v. Kampendahl*, 2002 WL 12997, at *6 (N.D. Ill. May 20, 2002) (applying Colorado UTSA).

[65] *Id.* at *6.

[66] *Buffets, Inc. v. Klinke*, 73 F.3d 965, 968-69 (9th Cir. 1996) (holding that recipes for staple dishes, such as BBQ chicken and macaroni and cheese, were not trade secrets); *In re Arthur Treachers Franchise Litigation*, 537 F. Supp. 311, 319 and 322 (E.D. Pa. 1982).

[67] *In re Arthur Treachers Franchise Litig.*, 537 F. Supp. 311, 322 (E.D. Pa. 1982).

[68] *Id.*

2. Methods of Doing Business

Methods of doing business are often at the heart of the value of a franchise system and have been the source of frequent litigation between franchisors and franchisees over the years. The *Gold Messenger* case from Colorado is illustrative. Gold Messenger was an advertising circular. After developing a comprehensive system for setting up and operating an advertising circular business, Gold Messenger began selling franchises.[69] The defendant's roommate and life partner became a franchisee and, as part of the franchise agreement, received the franchisor's operations manual. The operations manual detailed how to set up and operate a Gold Messenger franchise. The franchise agreement contained a covenant not to compete providing that, upon termination, the franchisee would not be permitted to compete directly or indirectly with Gold Messenger for three years and within 50 miles of the franchised territories.[70] After Gold Messenger terminated its franchisee's franchise agreement for nonpayment of royalties, the defendant began publishing a competing advertising circular distributed in roughly the same territory as he and the franchisee had distributed Gold Messenger. Gold Messenger sued, seeking to enjoin defendant's operation of a competing mailer.

Under Colorado law, noncompete provisions are prohibited with three exceptions—one of which is where the covenant not to compete is directed at the protection of trade secrets.[71] The defendant argued that this exception did not apply because the operations manual did not contain trade secrets. The court disagreed, holding that although the precise value of the manual was in dispute, it did provide an advantage over other competitors.[72] The court also noted that, while in possession of the confidential information in the manual, the defendant was able to produce successfully several issues of the competing mailer and also was paid to assist in the start up of another circular that was modeled on the competing mailer. Finally, the court noted the "substantial steps" taken by the franchisor to protect the operations manual, including copyrighting the manual[73] and requiring franchisees to execute franchise agreements acknowledging the confidentiality and value of the manual.[74] Accordingly, the court concluded that the confidential information in the operations manual constituted a trade secret.[75]

Not every franchise system is a trade secret, however. Courts have denied trade secret protection where the franchisor has not presented adequate evidence to show that the

---

[69] *Gold Messenger, Inc. v. McGuay*, 937 P.2d 907 (Colo. App. 1997).

[70] *Id.* at 909.

[71] COLO. REV. STAT. § 8-2-113(2) (West 2012).

[72] *Gold Messenger*, 937 P.2d at 911.

[73] Registration of a work with the Copyright Office is required for copyright protection for a work. There are three elements to registration: (1) a completed application, (2) payment of a fee, and (3) deposit of a copy of the work as to which protection is claimed. When copyrighted works contain trade secrets or confidential information, deposit of and public access to the copyrighted work would obviously defeat trade secret protection, because copyrighted materials are publicly accessible and therefore note secret. However, the Copyright Office has issued regulations permitting deposit of non-confidential portions of a work.

[74] *Id.*

[75] *Id.* Other examples of cases holding that a franchise system was a protected trade secret include *Tan-Line Studios, Inc. v. Bradley*, 1 U.S.P.Q.2d 2032, 2038 (E.D. Pa. 1986) (holding that "entire methodology for conducting a tanning studio" including methods of employee recruitment and training, studio layout, cash control, advertising, accounting, marketing, promotion and site selection that were not generally known in the industry constituted a trade secret) and *Smokenders, Inc. v. Smoke No More, inc.*, 184 U.S.P.Q. 309 (S.D. Fla. 1974) (holding that detailed step-by-step system for assisting people to quit smoking was a protectable trade secret).

procedure is unique within the relevant industry or based on specialized knowledge. Courts also deny protection where the efforts to preserve the secrecy of the procedure were inadequate. Another Colorado case, involving a frozen yogurt franchise system, illustrates this point. In *I Can't Believe It's Yogurt v. Gunn*,[76] the franchisor terminated the defendant's franchise agreements for failure to pay fees, after which the former franchisee continued to operate a store that sold frozen yogurt, used some of the same business systems and kept the same layout. Among other claims, the franchisor asserted a claim for misappropriation of trade secrets, claiming that its trade secrets were contained in the operations manual and included the entire "business system" of the store—including an allegedly strategic layout and design of the store, various accounting procedures, the proper use of yogurt machines, proper handling of yogurt mix, inventory management, interviewing and hiring practices, and selling techniques.[77]

After a bench trial, the court concluded that the franchisor failed to prove the existence of any protectable trade secret information. The court so held even though it accepted the general proposition that a franchisor's business system "can constitute a trade secret, even though individual components of such system may not qualify as such."[78] The court concluded that all of the information claimed to constitute trade secrets was either generally known or readily ascertainable.[79] The court discounted the testimony of the plaintiff's founder to the effect that the franchisor's business procedures gave his company a competitive advantage, citing the founder's testimony that he had not worked anywhere else since founding the company and that he did not know whether other businesses had similar procedures.[80] The court also noted that much of the information the franchisor claimed as a trade secret was taught in business school. The court further concluded that the franchisor's efforts to protect its trade secrets were inadequate. Although the franchise agreement contained confidentiality provisions, the franchisor's business procedures were disclosed to all people who attended its training, including managers and employees who were never required to sign a nondisclosure agreement. In addition, the franchisor divulged much of the claimed trade secret information—including products and recipes—through standard system publications without any statement that the information should remain confidential. Consequently, the court held that the franchisor failed to carry its burden on its trade secret claims.

3. Strategic Business Plans

Motor City Bagels, LLC v. The American Bagel Co.[81] involved a somewhat unusual situation in which the franchisee sued the franchisor for misappropriation of trade secrets in the form of the franchisee's business plan.[82] Before signing the franchise agreement, the

[76] *I Can't Believe It's Yogurt v. Gunn*, 1997 WL 599391 (D. Colo. Apr. 15, 1997).

[77] *Id*.

[78] *Id*. at *23.

[79] *Id*. at *22.

[80] *Id*.

[81] *Motor City Bagels, LLC v. The American Bagel* Co, 50 F. Supp. 2d 460, 478-81 (D. Md. 1999).

[82] The case is not the only one of a franchisee suing a franchisor for misappropriation, however. In *Camp Creek Hospitality Inns, Inc. v. Sheraton Franchise Corp.*, the franchisee claimed that the franchisor misappropriated the franchisee's information as to "occupancy levels, average daily rates, discounting policies, rate levels, long term contracts, marketing plans and operating expenses" and used this information to compete against the franchisee. 139 F.3d 1396 (11th Cir. 1998). Although the district court had granted summary judgment, concluding that the information was not a trade secret, the Eleventh Circuit reversed, holding that the franchisee had presented sufficient

franchisee had compiled an extensive business plan assessing the viability of operating the franchised restaurants, intending to use the plan as a way to secure investors in their franchises.[83] The plaintiff shared the plan with a representative of the franchisor, who asked if he could keep a copy. The franchisee consented on the condition that it not be shared with anyone else. The franchisee later discovered that many other prospective franchisees were provided with the business plan.

The court assessed whether the plan qualified as a trade secret under Maryland's version of the UTSA. The court noted that the plan contained some public information and facts ascertainable from the marketplace, but also contained "personal insights and analysis brought to bear through diligent research and by marshaling a large volume of information," the duplication of which "would be an onerous task."[84] Citing numerous cases, the court concluded that the extensive compilation of information and analysis in the business plan qualified it as a trade secret.[85] The court likewise held that the business plan derived value from its secrecy. However, the court concluded that the franchisee did not take adequate steps to protect the secrecy because it distributed the plan to more than fifteen potential investors, but could only produce proof that it obtained confidentiality agreements from five of them.[86]

4. Customer Lists and Information

"It is beyond dispute that frequently the single most valuable asset of an enterprise is the relationship it has developed with its customers."[87] As a general rule, customer lists and information can be protected as trade secrets (assuming value and reasonable measures to preserve secrecy were taken) where there is a restrictive covenant covering the customer list or information.[88] Nevertheless, a practitioner is advised to look closely at the applicable state law and the factual situation when customer lists are the trade secret his or her client seeks to protect. Indeed, some states expressly include customer lists and information in the definition of "trade secret,"[89] where others do not.[90] In some cases, courts engage in an analysis of whether the requirements for trade secret protection (*i.e.,* secrecy, value, and reasonable efforts to preserve confidentiality) have been satisfied. In other cases, courts have been content to rely on restrictive covenants between the franchisor and franchisee and assume that the information is a trade secret.

---

evidence that the information was a trade secret through expert testimony that the information was closely guarded in the industry (thus evidencing economic value) and that a competitor could not have compiled the information through legitimate means.

[83] *Motor City Bagels, LLC*, 50 F. Supp. 2d at 477.

[84] *Id*. at 479.

[85] *Id*.

[86] *Id*. at 480.

[87] *Milgrim* § 1.09[7] at 1-550.

[88] *See Milgrim* § 1.09[7][a][ii] ("[I]t is almost universal that a customer list which has some basis for a claim of secrecy can be protected by a restrictive covenant") (citing cases by jurisdiction).

[89] *See* Colorado UTSA, COLO. REV. STAT. ANN. § 7-74-102 (West 2007). Connecticut UTSA, CON. GEN. STAT. § 35-51 (West 2007); Georgia Trade Secrets Act, GA. CODE ANN. § 10-1-761 (West 2007).

[90] *See* California UTSA, CAL. CIV. CODE § 3426.1(West 2007); Kentucky UTSA, KY. Rev. Stat. Ann. § 365.880 (West 2006); Missouri UTSA, MO. REV. STAT. § 417.453 (2007).

American Express Financial Advisors, Inc. v. Yantis[91] is an example of the first approach. In that case, a former franchisee terminated his relationship with franchisor American Express and joined a competitor, taking with him customer information. American Express sued for breach of the franchise agreement, misappropriation of trade secrets and confidential information, and unfair competition, and sought a preliminary injunction to prevent the former franchisee from using confidential information. The confidential information at issue included customer lists and records (which included identifying information, investment history, investor suitability information and financial plans), know-how concerning methods of operation, and other financial information.[92]

For purposes of deciding preliminary injunctive relief, the court concluded that American Express was likely to succeed in showing that this information fell within the legal definition of a trade secret under Iowa law. First, the court concluded that American Express had shown the information derived economic value from not being generally known or readily ascertainable by proper means. The court noted in particular that the customer files contained information regarding the clients, their financial histories, and goals which would be helpful to a competitor and would require cost, time, and effort to duplicate. Second, the court concluded that American Express had taken sufficient efforts to guard the secrecy of the information by (1) requiring all franchisees to execute contracts designed to protect the information; (2) requiring franchisees to require any members of the franchisee's staff with access to franchisor confidential information or information about current or potential clients to sign a confidentiality agreement; (3) requiring that the franchisee not use confidential information in any way except as permitted to operate his franchised business during and after the term of the agreement; and (4) requiring franchisees to agree to post-termination restrictive covenants limiting the franchisee's ability to contact, solicit, or service American Express clients.

Jackson Hewitt Inc. v. Childress[93] is illustrative of the latter approach. There, the franchisee unilaterally terminated franchise agreements permitting him to operate tax return preparations businesses in various territories in Alabama using Jackson Hewitt's name and marks and its proprietary business methods and software. After termination, the former franchisee continued to operate a competing tax return preparation business from the same location as his former Jackson Hewitt franchised location and failed to return to Jackson Hewitt "trade secret, confidential and proprietary materials." These materials were alleged to include the identities of the customers served by the franchised business, and copies of their tax returns for the two prior tax seasons.

The court started by analyzing the franchise agreement. The court noted that the former franchisee had agreed, *inter alia*, that the identities of the customers served by the franchised location for the two preceding tax seasons were Jackson Hewitt's "trade secrets, confidential and proprietary information."[94] The franchisee agreed that the unauthorized use or disclosure of the trade secrets and confidential information would cause irreparable harm for which damages were an inadequate remedy. In a post-termination covenant, the franchisee agreed that, for a period of twenty-four months following termination, he would not "directly or indirectly prepare or electronically file individual tax returns, teach tax courses, offer [specific products] or own,

---

[91] *American Express Fin. Advisors, Inc v. Yantis*, *358* F. Supp. 2d 818 (N.D. Iowa 2005).

[92] *Id*. at 831.

[93] *Jackson Hewitt Inc v. Childress*, 2008 WL 199539 (D.N.J. Jan. 22, 2008).

[94] *Id*. at *2.

engage in, operate, [or[manage ... a Competing Tax Business" within a specific territory.[95] He also agreed not to disclose any of the franchisor's trade secrets, as defined in the franchise agreement, and consented to preliminary and permanent injunctive relief for violations.

In analyzing whether to grant injunctive relief, the court considered whether the covenant not to compete protected legitimate interests of the franchisor which—under New Jersey law—could include the protection of trade secrets, confidential information, and customer relationships.[96] The court did not engage in an extensive analysis of whether the information in question was a trade secret, relying instead on the provisions in the franchise agreement in which the defendant acknowledged that the information was a trade secret. The court emphasized that the former franchisee had acknowledged Jackson Hewitt's "customer relationships, trade secrets and confidential and proprietary information" were critical to the franchisee and "contractually acknowledged and reasonably anticipated" the injunctive relief that the franchisor sought.[97] Accordingly, the court granted the injunctive relief requested by the franchisor.

5. Planned promotional campaigns

Planned but not-yet-public advertising and marketing campaigns and plans related to new products or services can be protectable as trade secrets.[98] In *H&R Block Eastern Tax Services, Inc. v. Enchura*, an income tax preparation company brought suit against two former employees to prevent them from working for a competitor.[99] Shortly before leaving the company, the two employees attended a meeting at which they received a three ring notebook approximately three inches thick that contained a combination of publicly available information and information about client profiles, upcoming advertising campaigns, promotional plans, new services, financial date and projections and compensation and pricing plans. Most of the information related to advertising, promotions, new products, and pricing was to be publicly revealed at the beginning of the upcoming tax preparation busy season.

The court considered whether this material met the definition of a trade secret under Missouri's definition of the UTSA. [100] The court concluded that the publicly available information was not entitled to protection because it was "so elementary and obvious (*e.g.*, certain basic, business-oriented catch phrases" and the tax preparers desire to retain experienced tax preparers like the defendants) that there was "no competitive advantage gained from its

---

[95] *Id*.

[96] *Id*. (citations omitted).

[97] *Id*. at *7.

[98] *PepsiCo v. Redmond*, 54 F.3d 1262, 1265-66 (7th Cir. 1995) (affirming grant of preliminary injunction against inevitable disclosure of plaintiff's yet-to-be employed marketing plans, where plaintiff was a small competitor in the field relative to defendant); *Xantrex Tech., Inc. v. Advanced Energy Indus.*, 2008 U.S. Dist. LEXIS 41206, at *47 (D. Colo. May 23, 2008) (holding that new product development and detailed customer information likely to be found a trade secret supporting entry of preliminary injunction under Colorado UTSA); *LeJeune v. Coin Acceptors, Inc.*, 849 A.2d 461, 465 (Md. 2004) (holding that marketing methods and new product information, which were accessible only to employees of the company, were trade secrets); *H&R Block Eastern Tax Services, Inc. v. Enchura*, 122 F. Supp. 2d 1067 (W.D. Mo. 2000); *Merck & Co., Inc. v. Lyon,* 941 F. Supp. 1443 (M.D.N.C. 1996) (holding that trade secrets related to project launch dates of product line extensions were entitled to trade secret protection).

[99] *H&R Block Eastern Tax Services, Inc.*, 122 F. Supp. 2d 1067.

[100] *Id.* at 1073-74 (*citing* Mo. Rev. Stat. § 417.453(4)).

secrecy."[101] The court did, however, conclude that non-public information related to (1) details of planned advertising and marketing; (2) changes and additions to services offered to customers, and (3) compensation and pricing matters, met the definition of trade secrets.[102] Although the court permitted the former employees to work for the competitor, it placed restrictions on their activities, such as prohibiting them from working with the competitor's franchises in the employees' regions and enjoined them from revealing to their new employer information about plans related to advertising, marketing, and new products and services.[103]

6. Computer software

In *Rivendell Forest Prods., Ltd. v. Georgia-Pacific Corp.*, 28 F.3d 1042, 1046 (10th Cir. 1994), the Tenth Circuit overturned a district court decision that a collection of computer software elements already in the "public domain" could not qualify for trade secret protection. The software at issue consisted of "Quote Screen" applications for displaying lumber and freight prices. Several aspects of the *Rivendell* decision are noteworthy.

First, it is not entirely clear that the district court viewed a combination of public elements to be in and of itself devoid of protection. Its argument seemed to be that plaintiffs had not made a compelling argument as to *how* these elements combined into a protectable system. After all, the Mrs. Field's cookie recipe no doubt comprises known ingredients. By analogy, patent protection requires only a combination that is novel, has utility, and is "non-obvious." One distinguishing factor of a trade secret is that it rewards that which is "secret and of value," not who "got there first." The district court seemed willing to grant Rivendell its "lumber recipe" but wanted more of a "taste." The Tenth Circuit disagreed.

Second, the connection between a "secret" and software in the "public domain" depends upon the precise meaning of "public domain." Most software begins as human readable work product or source code—"the sweat of the programmer's brow." It may later be converted into a machine-readable form for actual use in the target environment, into non-human "object" or "executable" code. Typically, only the latter is supplied with commercial software. The purchaser or licensor is typically denied the source code physically and by license, unless an escrow arrangement has been made. By contrast, the "Open Source Movement" that started in the 1970s and became a market force in the 1990s seems to establish an alternative path of software development by making source code openly available through a far-flung community of developers to improve and correct the code, with the provision that its use must be accompanied by the appropriate licensing and usage provisions.

Taken together, the *Rivendell* decision and the Open Source Movement represent both an opportunity and a challenge to those commercial enterprises seeking protection for their proprietary methods. On the one hand, the past twenty years has seen widespread use of Open Source modules incorporated into commercial software. These modules are not truly "public domain" because they are based on a licensing model and have some restrictions on their use. At the same time, companies are often challenged to prove or disprove that the supposedly infringing elements of a commercial application are in fact built on Open Source

[101] *Id*. at 1074.

[102] *Id*.

[103] *Id*. at 1077.

components.[104] What makes *Rivendell* interesting is that the Tenth Circuit decision tells us that for the sake of trade secret protection, it matters little who actually wrote the modules, but how they were arranged and leveraged.

III. BEST PRACTICES FOR MAINTAINING ADEQUATE SECURITY

Maintaining adequate security in an enterprise is not a monolithic activity but requires a program combining policies and procedures, physical and technical measures, ongoing awareness, training, and re-evaluation.

Policies regarding information security may not strike one as novel, but they do establish the following:

- Elevate awareness that information security is an important element of company policy and promote that awareness in a structured, mission-critical fashion.

- Generally delineate the broad areas of information and behaviors that will be subject to the underlying security procedures, helping to establish the line between allowed "company" activities and unmanaged "personal" activities.

- Establish a flexible framework for potential new areas of security coverage in light of new technologies, employment and franchise paradigms, and marketing trends. For example, in the pre-commercial Internet era, it was not widely contemplated that massive amounts of company information could be transported outside its four walls *without* the use of physical media such as diskettes and tapes. Other challenges include a company's management and control of the now ubiquitous iPhones and other employee-owned personal devices when used to access corporate email servers.

A. Data Protection: It Starts With the Employees

From a procedural standpoint, employees are the main focal point of a sound security framework. Most losses of information, including data theft, corruption, and accidental deletion or disclosure can be traced back to inadequate employee training and awareness. The problem is exacerbated for many companies that have sought to reduce headcount through the use of contract employees, who must attain awareness of company security requirements in an expeditious and consistent manner. Other recent trends that have underscored the need for greater security include:

- Globalization, resulting in movement of data across international boundaries in the ordinary course of business.

[104] A troubling side effect of the Open Source movement are the steps involved in refuting a claim that allegedly infringing code is protected as Open Source. This activity necessitates a time-consuming search of all Open Source code, complicated by the "contamination" inherent in an Open Source / proprietary combination. Google Code Search, designed to help people search for Open Source code, was shut down on January 15, 2012, although alternatives exist such as koders.com, opensearch.krugle.org, grepcode.com, and antepedia.com. *See also* D'vorah Graeser, *The Benefits and Risks of Open Source Licensing*, ZDNET (Mar. 28, 2012), zdnet.com/news/the-benefits-and-risks-of-open-source-licensing/6354375.

- Greater mobility, including the near replacement of many desktop computers with laptops, the widespread access of corporate assets through other portable devices, and the intermingling of company information with personal information.

- Social networking applications that further erode the line between that which is public and private, and that between company and personal information.

- An increasingly sophisticated and far flung community of hackers and other cyber-criminals attacking the corporation from both inside the firewall and halfway around the world.

The company can effect these objectives through the establishment, promotion, and monitoring of several key instruments. Confidentiality agreements help manage the security relationship during and after the employment relationship by clearly delineating the protected subject matter and obligations of the employer. Employee manuals and usage policies make the policies actionable on a day-to-day basis and address actions that may be ambiguous. Examples include:

- Which electronic assets are actually "owned" by the company?

- What types of information must be encrypted before sending it out of the company?

- What categories of information can one share with others in the company, department, or workgroup?

- What geographical boundaries exist with respect to company information?

- Can one share his or her password or login information with a colleague?

- How is a business record defined within the company? How does one determine when items such as email messages are business records and ensure that they are properly classified, protected, made properly accessible, and retained? How does a litigation hold modify that behavior?

- How does one respond to potentially compromising actions of others that relate to information security?

- How must employees balance security requirements with convenience (for instance, writing a frequently changing password on a Post-It note)?

Of course, having answers to these questions is only as effective as an employee's having ready access to the answers. The procedures should be described and reinforced from new employee training through certifications on new equipment and applications and via ongoing monitoring and reviews. Reference materials can be placed online effectively if the number of "clicks" and layers is kept to a minimum. Prospective employees should undergo detailed background checks to preclude hiring the next Kevin Mitnick![105] By the same token, outgoing employees should undergo detailed exit procedures, including interviews and

[105] Formerly known as the "world's most wanted computer hacker."

reminders of obligations under confidentiality provisions. Exit procedures should take into account processes for separating company assets from personal (particularly on laptops), in a manner that does not involve surprise for either employer or employee. Employee performance reviews should also make security compliance a measured attribute.

B. Timely Audits

From time to time, the company should perform detailed audits of processes, repositories, and equipment. It should know which files and systems have been regularly accessed (and should not have been), and which lay dusty and cobwebbed. It should identify which systems have missing or long running passwords (such as the ever vulnerable Microsoft SQL Server "SA" account).[106] It should also audit the applications running on the network and desktop or laptop computers (easily done with a centralized systems management application). If employees are permitted by policy to install applications on their computers, the audit will indicate if they are managing their personal checkbooks or running a gambling parlor.[107]

C. What's A Record? (And Why Should I Care?)

One of the many challenges confronting corporations today is matching their records retention policies to the actual information storage containers and data types. Few companies have effectively developed methods to actually classify and file emails outside of imposing blanket inbox size and date restrictions which force users to make decisions about retention that directly affect security (such as dragging business emails into local "PST"[108] folders).

Some companies have adopted a practice of archiving *all* mail items into a giant third party repository, which itself can generate significant security and management risks. With the exception of businesses subject to SEC regulation or other requirements, companies should not be archiving information about weight loss pills or Caribbean time shares. As part of an overall security program, many vendors offer email filtering software to assist in identifying non-business correspondence and potential security threats.

Further, from a records retention standpoint, many companies have not made clear to their employees how to dispose of electronic and paper-based business information in the appropriate time frame and in the approved manner ("What about printouts?" "Which copy is the official record?" "Should one print out the version to be archived?" "What about the earlier versions attached to emails?" "How does one disposition files in shared directories?"). This potentially un-dispositioned information poses a security risk and retention liability.

D. Companies Must Exert Ownership over Their Digital Assets

Where applicable, the company should make use of tools such as document management and source code management applications to retain, centralize, control access, and audit company documents and intellectual property assets. These tools manage the overall

---

[106] The "System Administrator" account on Microsoft's popular enterprise database management system.

[107] In one legendary industry story, a major computing vendor uncovered a server hidden under the floorboards in its offices running an illicit business through the company's network.

[108] "Personal Storage Tables"—a container for Microsoft email that typically lives outside the central network on a user's hard drive. It is typically used to free up central mail server space or to transport groups of emails, but results in a loss of centralized oversight and control over the messages.

information lifecycle. They remove decisions about where to store and how to name documents. They apply retention automatically without the need for an annual records "clean-out" day. They also enable roles to be identified and distinguished between multiple authors, typists, and other contributors.

The larger context beyond authorship is that the company must understand which assets it owns and who controls them—not just for documents but for equipment, software licenses, program or source code, and structured data.[109] Certain intellectual property assets such as source code can be made subject to escrow agreements to allow ownership without access, potentially addressing both licensing and security concerns.

Numerous cases have arisen of former employees being accused of spiriting away customer databases to new ventures, with the defense being that the information was available in the public domain. The rise of open and relational database management systems started on the mainframe in the 1970s but took off in the era of "client/server" computing in which the computing responsibilities were split across multiple computers. The byproduct of this capability is the ability to bypass the "front end" application and its limited security, exposing the "back end" database to report writers, querying tools, and boundless opportunities for data corruption, destruction, and theft.

E. Network Security Is an Onion

It is helpful to view the corporate network as an onion with many layers of potential security protection. Those layers include physical, social, and data levels.

As mentioned above, data can "walk out" of an enterprise in ways never contemplated by locked doors, yet the need for physical security is greater than ever. The use of physical key cards, access logs (especially to server rooms and data centers), cameras, time restrictions, human eyes, building passes, periodic inventories, and locked doors remains paramount. Some measure relate to accidental damage (some of us remember the 1979 "Pepsi Syndrome" sketch on *Saturday Night Live* involving a nuclear meltdown resulting from a spilled carbonated beverage). As a result, modern server rooms and data centers have environmental controls that include HVAC, fire suppression, backup power, and replicated backup sites to protect and secure corporate data.

Unfortunately, some production server rooms double as equipment storage or have work areas where IT employees perform tasks in unnecessarily close proximity to critical operational data. Backup tapes are carried in and out every day by a courier service, which may present a security risk. Computers can be secured so that they can only be logged into at certain times of the week by certain people; ports and drives can be disabled or removed to minimize unauthorized data movement. Server rooms and data centers should have inconspicuous signage and location. Finally, an asset tracking system can manage which resources are assigned to which employees and enable periodic audits.

Employees themselves can subject the company to significant risk through unintended actions. Passwords can be stuck on monitors or provided to temporary employees. Information

[109] *See* discussion of the *Rivendell* case, *supra* Section II.B.6.

can be elicited through "phishing" phone calls, emails, and other "social engineering" techniques. Web links can lead to rogue programs implanted in the corporate network.[110]

F. Building Layers of Data Protection

The company can and should build layers of protection around its physical and intellectual property assets. The layers should include end user responsibility in addition to a consistent, structured, but flexible framework between the various departments of Information Technology, Data Security, Risk Management, the Records Office, Legal, company management, and the business units themselves. With the level of interconnected commerce in many businesses, outside suppliers and other third parties must participate in the security framework. The company should develop consistent practices for managing the procurement and lifecycle of end user and centralized resources, including its software change management practices,[111] anti-virus updates, password controls and changes, data "wiping" practices, and desktop security "policies."[112] Many corporations used to the corporate controls inherent in BlackBerry devices are finding ways to exert authority and control over Apple and Android devices to require passwords, prevent certain actions, and allow remote data wiping.

Other access controls are inherently network-based. The network can keep logs of access activity, security events, and application usage that can be traced to a particular machine. These logs will just sit quietly on the server without a program of active analysis and pattern detection. Passwords and security can be enforced at login to the network, when accessing specific applications such as HR and email, and when accessing specific data storage locations and databases. Nonetheless, a multiplicity of passwords can also pose a security risk, and modern network operating systems such as Microsoft Windows seek to minimize the number of passwords by creating a central listing called the "Active Directory" that tracks a user's "bundle" of access rights in one place.

G. It's Raining Data into The Cloud

Enforcing security for data sent over the Internet bedevils many companies. Hosted cloud services such as DropBox and third party email services provide a "shadow" to the corporate network, allowing employees and third parties to transmit information and store corporate data in places not easily audited. To some extent, network services can monitor Internet traffic, preclude visits to certain Web sites, prevent certain types of attachments from being mailed or received, and strip hidden "metadata" from outbound Office documents. Best practices also may include control of electronic signatures, scrubbing metadata from Office

---

[110] It was revealed that similar techniques were used to implant data mining and equipment destroying viruses like Stuxnet and Flame in Iranian computer systems. Thomas Erdbrink, *Iran Confirms Attack by Virus That Collects Information*, N.Y. TIMES, (May 29, 2012), (http://www.nytimes.com/2012/05/30/world/middleeast/iran-confirms-cyber-attack-by-new-virus-called-flame.html).

[111] Examples include software "patching," updates, rollbacks, migrations, configuration, and customization. "Patching" and updates refer to introducing newer versions of software to fix problems or add features. Without proper testing, new and unforeseen problems can arise, leading to the necessity of additional patching or performing a disruptive "rollback" to an earlier version. Further, when the underlying data storage structures change for a business application (such as allocating ten spaces for a zip code as opposed to five), the data must be "migrated," creating a business risk without the proper controls and safeguards.

[112] In Microsoft parlance, "policies" refer to the group controls that regulate whether users can perform such actions as install new software, add icons, use USB or optical devices, connect to certain resources, write to local storage, create PST files, and access the "command" prompt.

documents or allowing only PDFs to be sent (with *copy* and *paste* disabled), but user bad intentions cannot be "legislated away" simply through technology means.

From a remote access standpoint, logging in as a "terminal" using tools such as Citrix technology or to a Web portal have built in security layers that insulate the remote user from direct access to network resources. On the other hand, certain applications require the remote computer to truly log in to the network as if the user was physically in the office. Typically these connections are made using a "VPN" or virtual private network technology that passes private corporate information over the public Internet. Because of the potential security risk when a remote user has unfettered access to in-house resources, VPN access is built on a highly sophisticated security scheme that may involve such methods as "tokens" stored on credit card-like devices. Nonetheless, even VPN connections require constant maintenance and vigilance to minimize network exposure. Although a deep examination of end user activity formerly required a site visit to the computer and an obtrusive examination using a forensic examiner with a specialized toolkit, the current generation of corporate security tools enables data search and forensic level acquisition unobtrusively from a central location worldwide, without "law enforcement" level training.

The coordinated use of these policies, procedures, and tools in an organization yield the "perimeter security" to safeguard the network and its data. For many corporations, creating the role of "data security officer" and seeking specialized assistance and audits may round out the security program.

H. Contract Provisions

A claim for misappropriation of trade secrets is one that sounds in tort—whether common law or statutory—and is a claim that can be asserted even in the absence of a written agreement prohibiting the use or disclosure of trade secret information. The existence of a contract may, however, give the owner of confidential information a claim for breach of contract for improper use or disclosure of information, in addition to a tort claim. Furthermore, the presence of contractual provisions in a franchise agreement defining the franchisor's trade secrets and placing limits and requirements on their use within the scope of the franchise relationship can strengthen a claim for misappropriation of trade secrets.[113] Thus, every franchisor should consider the various contractual mechanisms for protecting trade secrets.

A franchise agreement should define or identify in general terms things about the system that the franchisor considers to be trade secrets and confidential information. The definition should be broad, but still fitted to the trade secrets of the particular system.[114] In addition, in the franchise agreement, the franchisor should consider requiring acknowledgments from franchisee that (1) trade secrets and confidential information have been developed and/or are

[113] *Kodekey Elec., Inc. v. Mechanex Corp.*, 486 F.2d 449 (10th Cir. 1973) (applying Colorado law and finding agreement by defendants not to disclose information obtained, not to compete, and not to use information obtained detrimentally was acknowledgement of fact that information was a trade secret); *Jackson Hewitt, Inc. v Childress*, 2008 WL 199539 (D.N.J. Jan. 22, 2008) (granting preliminary injunction against franchisee enjoining competition where franchisee "contractually acknowledged and reasonably anticipated" the injunctive relief sought by the franchisor), *Gold Messenger*, 937 P.2d at 912 (noting that terms of the agreement that declared confidential information to be "trade secrets").

[114] *Frosty Bites, Inc. v. Dippin' Dots, Inc.*, 369 F.3d 1197 (11th Cir. 2004) (holding that confidentiality agreements that franchisor required dealers and franchisees to sign were deficient in that they did not identify what constituted the trade secrets).

owned by franchisor and are provided as part of the franchise system or training and standards; (2) the subject information is not generally known in the industry and could not be developed without great time/expense; and (3) the franchisee may have access to trade secrets and those trade secrets will provide the franchisee with a competitive advantage.[115]

Examples of these types of clauses can be found in the *Gold Messenger*[116] case, discussed *supra*, in which the Colorado Court of Appeals found that trade secrets existed. There, franchise agreement contained the following language:

> WHEREAS, Franchisor is the owner of certain techniques, know-how, trade secrets and procedures (the Know-How) which are used in connection with Franchisor's Controlled Circulation Advertising Publication business and Franchisor's Franchisees;
>
> WHEREAS, Franchisor [has] developed a unique system for operating [the] business, including business forms, bookkeeping and accounting materials and techniques, management and control systems, and, in general, a style, system, technique and method of business operation . . .
>
> WHEREAS, Franchisee recognizes that it does not currently have the expertise contained in the developments as stated above and desires to use those developments pursuant to a franchise agreement.

Though the language broadly defines what the franchisor viewed as its trade secrets, it is also sufficiently specific so that the categories of information the franchisor believed to be trade secrets—including know how and systems—are identifiable. It also states that the franchisor developed and owns the information and the franchisee recognizes that it did not have the expertise to which it would be given access under the franchise agreement. This language was key to the *Gold Messenger* court's conclusion that trade secrets existed.[117]

In addition, the franchisor should stress the importance of maintaining secrecy in the franchise agreement and consider including provisions that restrict unauthorized use and disclosure of the franchisor's trade secrets. As discussed above, franchisors who do not limit access of franchisee employees to trade secrets do so at their peril.[118] The *I Can't Believe it's Yogurt* case teaches that franchisors should require the franchisee to have every employee who will be permitted access to the franchisor's trade secrets and confidential information execute an employment agreement containing appropriate restrictive covenants to protect the information. The franchisor should also consider including language explicitly allowing the franchisor to enforce the agreements against the franchisee's employees.

---

[115] *Gold Messenger*, 937 P.2d at 910 (quoting with approval portions of franchise agreement in which franchisee acknowledged that franchisor owned trade secrets).

[116] *Id.*

[117] *Id.* at 911-12; *See also American Express Fin. Advisors, Inc. v. Yantis*, 358 F. Supp. 2d 818, 821-825 (quoting extensively from franchise agreement).

[118] *See I Can't Believe it's Yogurt*, 1997 WL 599391 (D. Colo. Apr. 15, 1997); *Arthur Treachers*, 537 F. Supp. 311.

Other system documents can provide franchisors with opportunities to protect—or undermine—the protection of system trade secrets. For example, operations manuals should provide specific guidelines for protecting the secrecy, including:

- Limiting disclosure of information to franchisee employees with a need to know the information to be able to perform their job duties.

- Requiring physical security measures, such as limitations on physical and electronic access to trade secret information.

- Requiring exit procedures for franchisee employees with access to trade secret information.

- Requiring the franchisee to train employees on what is trade secret and confidential information and employee responsibilities to protect the information.

Finally, the franchisor should take other reasonable steps to preserve the secrecy of trade secret and confidential information more broadly within the system. System materials other than the manual containing confidential information should be clearly marked as such, and should be distributed only to those individuals with a need to know and who execute confidentiality agreements. In addition, the franchisor should avoid disclosing its trade secrets in public materials, such as in its FDD, in its marketing or promotional materials, or in advertising.[119]

IV. GONE BUT NOT FORGOTTEN: BEST PRACTICES FOR DEALING WITH DEPARTING EMPLOYEES AND FRANCHISEES

A. Exit Interviews With Departing Employees and Franchisees

Regardless of whether an employee or franchisee is leaving to work for a competitor or is merely being let go, the fact remains that departing employees and franchisees are one of the major sources of "leakage." Rarely will an "exit interview" produce a confession that a departing employee or franchisee has absconded or intends to abscond with the franchisor's trade secrets. Still, conducting such an interview is a recommended "best practice." Of course, there is always the possibility that a departing employee or franchisee will let slip some critical piece of information. Even if that does not happen, conducting an exit interview creates a record that should put the franchisor on more solid ground if, for example, it becomes necessary to seek preliminary injunctive relief against the departing employee or franchisee.

As part of the exit interview process, the franchisor should review its confidentiality policies and procedures (including any post-term covenants not to compete) with the departing employee or franchisee. Upon the conclusion of the exit interview, the departing employee or franchisee should be asked to sign a written acknowledgment of receipt of these policies and procedures and written certification of compliance. Needless to say, a refusal to sign may raise some "red flags" about the intentions of the departing employee or franchisee. Even if the departing employee or franchisee certifies compliance, with trade secret protection—as with arms control—"trust but verify" is a best practice. As set forth below under "Forensic Verification," a computer forensic expert may be able to determine the extent to the which a

[119] *See Aerospace America vs. Abatement Technologies, Inc.*, 738 F. Supp. 1061 (E.D. Mich. 1990).

departing employee or franchisee has misappropriated trade secrets or made plans to use them for the benefit of a competitor. Under certain circumstances, having such an examination conducted may be worth doing sooner rather than later. In circumstances where there does not seem to be any cause for immediate alarm, another possibility is to create a "clone" of the departing employee's or franchisee's computer that can be examined at a later date by a computer forensic expert if the circumstances suggest the need to do so.

B. Monitoring and Self-Help

Computer forensics experts can and should be retained to determine whether files were accessed, downloaded, or printed by employees or franchisees suspected of misappropriating trade secrets. As part of this forensic examination, the email history of the employee or franchisee in question should be reviewed to determine whether franchise system trade secrets have been the subject of suspicious email activity. Although the employee or franchisee may not have been brazen enough to email the trade secrets in question directly to a competitor, other email transmissions may be suspect. For example, an email to a home computer—especially when the employee or franchisee is about to depart—may not have had a legitimate purpose. Wrongdoers often try to "cover their tracks" by deleting certain files. These efforts are often unsuccessful, however, because computer forensic experts can often recover files that the wrongdoer attempted to delete. Not every departure of an employee or franchisee may justify the expense of a full-fledged forensic examination. Sometimes, however, a former employee or franchisee comes under suspicion long after departing. One relatively inexpensive best practice is to "clone" the computer hard drives of ***all*** departing employees and franchisees so that—if it later becomes necessary—a forensic examination can be conducted in the future.

Particularly with employees, monitoring may well run afoul of their "reasonable expectations of privacy"—unless the franchisor has expressly preserved the right to do so. The franchisor's written policies and procedures should therefore make clear that computer and telephone traffic may be monitored. These procedures should be the subject of periodic reminders. Ideally, employees and franchisees should be required to give written consent to monitoring.

One obvious method of self-help is a user log-in system with passwords to ensure that access is limited. If the franchisor's trade secrets include computer software, many software developers imbed disabling code a/k/a "logic bombs." Disabling code is designed to ensure that the software will work only on designated machines. Some disabling code may even cause malfunction if the software is used on non-designated machines. A franchisor that engages in this type of self-help should disclose the fact that such a device is in use and warn any potential users of any possible malfunction in the computer system if the software is not used in the proper manner. In this regard, implantation of "logic bombs" without disclosure to and consent by the licensee may be actionable as a "computer crime." For example, the case of *Roller Bearing Co. of America, Inc. v. American Software, Inc.*,[120] involved a dispute over an "upgrade fee" for the relocation of software. The licensed software contained an undisclosed "logic bomb" known as an authorization key. The licensee hired an independent consultant to "work around" the authorization key. The licensor's failure to disclose the required authorization key, the district court held, was actionable under the federal Computer Fraud and Abuse Act and the Connecticut Computer Crimes Act.

[120] Case No. 3:07-cv-01516 (D. Conn. March 23, 2010). *See also Roller Bearing Co. of Am., Inc. v. Am. Software, Inc.*, 570 F. Supp. 2d 376 (D. Conn. 2008).

C. Forensic Verification

There are occasions where it makes sense for a company to retain law enforcement-level resources for immediate response. One of those cases involves an examination of alleged employee behavior using forensic verification. A competent computer forensic expert can examine an employee's electronic materials and arrive at certain conclusions, prove or disprove certain hypotheses, and raise other issues about that employee's actions. These actions can include logging in, copying or accessing material, printing, erasing/wiping files, visiting Web sites, attaching equipment, and transmitting information. The forensic examination can tell a story or create a narrative centered around: What did the subject do and when?

Forensic verification can also be used for exculpatory purposes, showing intermediate mishandling measures. Woe to the company whose file listing for an employee who surrendered his or her computer for preservation in 2011 shows files with an access date from 2012. In their eagerness to search for bad behavior, lawyers and corporate IT representatives can easily spoliate a computer hard drive simply by turning it on and running a search. Forensic examiners can perform "imaging" of a hard drive, thumb drive, phone, or PDA, to provide a legally defensible point-in-time record of the media. They can make use of "hash values,"[121] "write blockers,"[122] and other methods to ensure chain of custody and demonstrate that no "tampering with the crime scene" has occurred.

D. Considerations for Windows-Based Computers

On a typical Windows-based business workstation, the forensic examiner has numerous non-obvious methods to discern past behavior, although their traces can deteriorate over time. Files that have been erased can be partially or fully recovered. The Windows Recycle Bin provides a temporary storage location for certain deleted files, which can be exculpatory or helpful to the user as well. A hidden catalogue of information known as "the Registry" provides a storehouse of information, both helpful and potentially hurtful, as to applications and devices installed and system changes made. Various files known as "desktop.ini" can materialize merely through a user traversing a set of folders.

Although the Windows file system generally tracks dates that include creation, modification, and last access, the latter is notoriously unreliable and can be changed without an actual file being opened. Creation date can reflect the date a file was copied to a location rather than its actual creation. And all are subject to the vagaries of how the system clock is maintained and the relevant time zone. Many other indicia are left behind when a Web site is visited, a password is entered, or a CD is burned. Even activity on Web-based email systems can be discerned by the electronic "droppings" left behind.

E. Effective Use of Forensic Experts

Through the techniques described above, a forensic expert can tell the story of "who did what when." The expert can preserve evidence of both wrongdoing and reveal exculpatory information. In the context of the employment lifecycle, the expert can provide both proactive measures ("Is the network secure?" "Who is sending information offsite?") and reactive

[121] A mathematically-generated sequence of numbers whose subsequent match confirms that data was not altered.

[122] A physical device that prevents data from being altered while an examiner accesses the media.

investigations ("Does this employee have unauthorized information?" "Is this employee engaged in illicit behavior?"). In a larger sense, the examiner can recover lost information, help "sift out" personal data or ownership rights between companies (helping to uncover, for example, whether or not business data has moved inappropriately from one company to another). The competent forensic can understand and ferret out human behavior and lead the team to an appropriate conclusion. Finally, he or she can accomplish these objectives while demonstrating consistent, court approved methods, tools, and testimony.

V. LOST IN CYBERSPACE? MAINTAINING TRADE SECRET PROTECTION IN THE INTERNET AGE

A. Effect of Posting on the Internet on Trade Secret Protection

Whether inadvertent or deliberate, the posting of trade secrets on the Internet may destroy their status as such. In this regard, deliberate posting may often occur for the very purpose of destroying trade secret protection. The actor may be a disgruntled former employee or franchisee or a labor union, for example. Early cases suggested that posting on the Internet automatically destroyed trade secret protection. More recent cases, however, seem to have adopted a more nuanced view. At least some of the more recent cases suggest the possibility that—depending upon the facts and circumstances—a franchisor whose trade secrets have been posted on the internet ***may*** be able to argue successfully that trade secret protection has not been lost.

1. The Early View

In two federal court cases involving the Church of Scientology, the fact that the Church's trade secrets had been posted on the Internet meant that trade secret protection was lost.[123] The *Netcom* and *Lerma* decisions are particularly significant for franchising for three reasons.

First, the Church of Scientology—through its affiliate, the Religious Technology Center—operates very much like a franchise. Indeed, the Church derives substantial licensing revenues from the trade secrets at issue. These trade secrets are the "Advanced Technology Works" used by parishioners to achieve greater spiritual awareness and freedom.

Second, there was no question that the Church of Scientology had employed adequate security measures. These included "use of locked cabinets, safes, logging and identification of the materials, availability of the materials at only a handful of sites worldwide, electronic sensors attached to documents, locked briefcases for transporting works, alarms, photo identifications, security personnel, and confidentiality agreements for all those given access parishioners themselves were subject to confidentiality agreements whereby they "are required to maintain the secrecy of the materials."[124]

Third, the result—loss of trade secret protection—was not altered by the fact that the trade secrets had been misappropriated and then posted on the Internet by a disgruntled former Church of Scientology minister.

---

[123] *Religious Tech. Ctr. v. Netcom On-Line Communication Servs.* 923 F. Supp. 1231 (N.D. Ca. 1995) ("*Netcom*"); *Religious Tech. Ctr. v. Lerma*, 908 F. Supp. 1362 (E.D. Va. 1995) ("*Lerma*").

[124] *Netcom*, 923 F. Supp. at 1254, n. 25.

The *Netcom* and *Lerma* decisions both stand for the proposition that—regardless of whether the original posting on the Internet was wrongful—those who subsequently access the material are no longer misappropriating trade secrets. In *Netcom*, the federal court in San Francisco observed: "evidence that another individual has put the alleged trade secrets into the public domain prevents RTC from further enforcing its trade secret rights in those materials."[125] Similarly, in *Lerma*, the federal court in Alexandria, Virginia stated:

> Once a trade secret is posted on the Internet, it is effectively part of the public domain, impossible to retrieve. Although the person who originally posted a trade secret on the Internet may be liable for trade secret misappropriation, the party who merely down loads Internet information cannot be liable for misappropriation because there is no misconduct involved in interacting with the Internet.

Lerma, 908 F. Supp. at 1368.

2. More Recent Cases: Fact-Specific Approach

Over time, the bright-line rule of *Netcom* and *Lerma* that posting on the Internet automatically destroys trade secret protection has become somewhat blurred. More recent cases have held that trade secret protection may not be lost notwithstanding publication on the Internet ***if*** publication is "sufficiently obscure or transient or otherwise limited so that it does not become generally known to … potential competitors."[126] Key facts critical to this determination include the following:

- How long was it posted?
- How promptly did the owner act?
- Who saw it?
- How accessible and popular are the site?
- Where does it show up in response to search engine queries?
- How much was disclosed?

B. Transmission of Trade Secrets By Email

Conceptually, the transmission of trade secrets by email raises some of the same issues as posting on the Internet. The most obvious difference, of course, is that email transmissions are typically directed to and intended for certain identified recipients as opposed to being generally accessible. Whether the fact that trade secrets have been transmitted via email destroys their protected status depends—like any trade secret—upon the reasonableness of the security measures.

---

[125] *Id.* at 1256 (footnotes omitted).

[126] *DVD Copy Control Ass'n v. Bunner,* 10 Cal. Rptr. 3d 185 (Cal. Ct. App. 2004).

To determine the reasonableness of the franchisor's security measures, courts consider the following:

- "the existence or absence of an express agreement restricting disclosure;"
- "the nature and extent of security precautions taken by the [franchisor] to prevent acquisition of the information by unauthorized third parties;"
- "the circumstances under which the information was disclosed ... to the extent they give rise to a reasonable inference that further disclosure, without the consent of the [franchisor], is prohibited; and"
- "the degree to which the information has been placed in the public domain or rendered 'readily ascertainable'."[127]

Reasonable security measures include the following:

- written agreements with franchisees to maintain confidentiality.
- confidentiality notice on the trade secrets themselves and in any electronic mail messages by which the trade secrets are transmitted;
- encryption of e-mail messages to prevent unauthorized access; and
- prompt measures to retrieve any trade secrets that have been disclosed inadvertently and to pursue anyone guilty of their misappropriation.

In the age of the Internet, it seems impractical to refrain from permitting franchisees to obtain trade secrets via the internet if not email. Ways of balancing the need for trade secret protection with commercial reality can include—in addition to the foregoing measures—having a secure email system and/or portal that provides an extra layer of trade secret protection.

C. Other Avenues For Protection: Computer Crimes Laws

No matter how "reasonable" the franchisor's security measures, the fact that a "hacker" has gained access to them raises the very real possibility that the franchisor has no viable cause of action for misappropriation of trade secrets. Although "hacking" would not constitute access by "proper means," the fact that a hacker was successful calls into question the reasonableness of the franchisor's security measures. Thus, the franchisor may not be able to meet its burden of proving that its trade secrets have been "the subject of efforts that are reasonable under the circumstances to maintain [their] secrecy."[128]

No matter how reasonable the security measures employed, the *Netcom* and *Lerma* decisions stand as powerful reminders that—once disclosed—trade secrets may no longer be trade secrets.

---

[127] *Baystate Techs. v. Bentley Sys.*, 946 F. Supp. 1079, 1092 (D. Mass. 1996).

[128] UTSA § 1(4).

Therefore, an *ex post facto* action for misappropriation of trade secrets may not be the most effective remedy for hacking. At both the federal and state levels, so-called "computer crimes" laws may provide effective relief without the need to establish the existence and maintenance of trade secret protection. The use of computer crimes statutes is discussed at length in **Section VI.B**.

VI. PURSUING WRONGDOERS—HOPEFULLY BEFORE IT IS TOO LATE

A. Preliminary Injunctions

1. The Only Effective Remedy?

Regardless of whether an injunction is the ***only*** effective remedy, it is in most circumstances the most effective remedy. Under the *Restatement*, "a defendant's continuing or threatened use or disclosure of a trade secret normally justifies an award of injunctive relief."[129] Indeed, where a trade secret has not yet been disclosed or used, an injunction may be the ***only*** appropriate remedy.[130] In addition to prohibitory injunctions, provision of complete relief may necessitate an affirmative injunction requiring the return of any documents, drawings, or embodiments of the trade secrets and the assignment of any patents based on the appropriated information.[131]

2. Preservation Of The Status Quo

A primary purpose of preliminary injunctive relief is to preserve the status quo pending trial. The status quo to be preserved by a preliminary injunction is the "last peaceable uncontested status before the dispute arose" pending the resolution of the merits.[132] Thus, the fact that the party opposing injunctive relief sought is already misappropriating trade secrets does not mean that a preliminary injunction should be denied on the grounds that the injunction would upset rather than preserve the status quo. This is consistent with the rationale for preliminary injunctive relief: prevention of irreparable injury pending trial.[133] However, the fact that trade secrets have already been disseminated may mean that preliminary injunctive relief is not available, as previously discussed.

3. Notice Requirements

Consistent with the Due Process Clause, the Federal Rules of Civil Procedure generally require notice to the adverse party before a preliminary injunction will issue. *See* Fed. R. Civ. P. 65(a)(1), which provides that "[n]o preliminary injunction shall be issued without notice to the adverse party." However, the Federal Rules do contemplate that an *ex parte* temporary restraining order of limited duration may be entered under certain circumstances.[134] In addition, federal laws protecting other forms of intellectual property provide for *ex parte* seizure orders

---

[129] RESTATEMENT (THIRD) UNFAIR COMPETITION § 44 at 500.

[130] *Id*.

[131] *Id.*, cmt. c at 500.

[132] *See, e.g., Richmond Med. Ctr. for Women v. Gilmore*, 11 F. Supp. 2d 795, 828 (E.D. Va. 1998). *See also Stemple v. Bd. of Educ. of Prince George's County*, 623 F.2d 893, 898 (4th Cir. 1980).

[133] *See*, *e.g.*, *Canal Authority of Florida v. Callaway*, 489 F.2d 567, 576 (5th Cir. 1974).

[134] Fed. R. Civ. P. 65(b).

under certain circumstances. For example, the federal trademark statute, the Lanham Act, contains special provisions for *ex parte* seizure orders with respect to counterfeit marks.[135] The Copyright Act authorizes temporary injunctive relief,[136] impoundment of infringing articles[137] and—in the case of federal criminal prosecutions—seizure and forfeiture.[138]

At the federal level, there is no comparable statute allowing a private right of action for misappropriation of trade secrets. However, the combination of the Federal Rules of Civil Procedure and state law can be used to accomplish the same result. As previously discussed, Fed. R. Civ. P. 65(b) does specify circumstances under which *ex parte* temporary injunctive relief is warranted. In addition, Fed. R. Civ. P. 64 provides that litigants in federal court are afforded the remedies for the seizure of property provided by the law of the State in which the federal court is located. These state law remedies include those available under state replevin statutes, which can be used in conjunction with Federal Rule 64 to obtain the return of trade secrets.[139]

These state law remedies also include those available under trade secret law. The Uniform Trade Secrets Act specifically authorizes mandatory injunctions requiring the return of all tangible embodiments of the trade secrets, as does the Restatement.[140]

4. Expedited Trial As An Alternative To Preliminary Injunctive Relief

If the parties consent to an expedited trial on the merits, the consent order can and should also include a provision whereby the parties agree to preserve the status quo pending trial. The Federal Rules also contemplate motions for expedited discovery.[141] In addition, the Federal Rules specifically allow the preliminary injunction hearing to be consolidated with the trial on the merits.[142]

5. Bond Requirement

Rule 65(c) expressly provides as follows:

> No restraining order or preliminary injunction shall issue except upon the giving of ***security*** by the applicant, in such sum as the court deems proper, ***for the payment of such costs and damages as may be incurred or suffered by any party who is found to have been wrongfully enjoined or restrained***. No such security shall be required of the United States or of any officer or agency thereof.

---

[135] *See* 15 U.S.C. § 116(d).

[136] 17 U.S.C. § 502.

[137] *Id*. § 503.

[138] *Id*. § 509.

[139] *Testerion v. Skoog*, 602 F. Supp. 578 (D. Minn. 1984).

[140] UTSA § 2(c); RESTATEMENT (THIRD) UNFAIR COMPETITION § 44, cmt. (e) at 503.

[141] *See* Fed. R. Civ. P. 26(d) (*Timing and Sequence of Discovery*).

[142] Fed. R. Civ. P. 65(a)(2).

6. Required Provisions

Rule 65(d) requires that a TRO or preliminary injunction: "set forth the reasons for its issuance," "be specific in terms," and "describe in reasonable detail, and not by reference to the complaint or other document, the act or acts sought to be restrained."[143] In other words, a prohibition against using or disclosing trade secrets is too vague and too broad. The moving party should submit a proposed preliminary injunction order, findings of fact, and conclusions of law.

7. Persons Bound By Injunction

Once preliminary injunctive relief has been entered, the order "is binding only upon the parties to the action, their officers, agents, servants, employees, and attorneys, and upon those persons in active concert or participation with them who receive actual notice of the order by personal service or otherwise."[144] To expand the reach of the injunction beyond the enjoined parties, the party obtaining the injunction can and should serve copies upon "those persons in active concert or participation with them."

8. Discretionary Nature of Preliminary Injunctions

The federal courts enjoy considerable discretion whether to grant preliminary injunctive relief.[145] As a result, certain "intangible" factors—including the credibility and reasonableness of witnesses, parties, and their counsel—can help tip the balance in favor of one party or another. In addition, the court can exercise its discretion so that the preliminary injunction is specifically tailored to ensure that no unauthorized disclosure of trade secrets occurs.

B. Federal and State Computer Crime Laws

1. Overview

At both the federal and state level, there are statutes enacted specifically to prohibit "hacking" and other so-called "computer crimes"—including unauthorized access to and disclosure of communications that have been stored electronically (such as voicemail and email). Depending upon the circumstances, such statutes may provide a more effective remedy than what is available for more traditional, "low tech" methods of trade secret misappropriation. To prevail, the franchisor need not prove the existence of trade secrets. As previously discussed, the fact that a "hacker" was successful makes it more difficult for the franchisor to establish the reasonableness of its security measures and that trade secret protection has not been lost. Depending upon the location of the Internet service provider and the Web site or computer that was improperly accessed, it may be possible to establish jurisdiction in a forum that is more convenient or advantageous. Such statutes may make it easier to seal all or part of the record so that competitors, customers, and the news media do not learn of the dispute or at least the means by which security was broken.

---

[143] Fed. R. Civ. P. 65(d).

[144] Fed. R. Civ. P. 65(d).

[145] *Deckert v. Independence Shares Corp.*, 311 U.S. 282, 290 (1940).

2. Federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA")

CFAA prohibits intentional access to computer without authorization, or beyond the scope of any authority. Damages recoverable must be greater than $5,000 but can be claimed for "any reasonable cost to any victim, including" the "cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense" and "any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[146] CFAA defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information."[147]

The scope of conduct actionable under CFAA is potentially quite broad. Its viability as an alternate means of recovery for misappropriation of trade secrets may be limited in some jurisdictions, however, by two lines of authority putting a judicial gloss on the scope of CFAA. The first addresses the extent to which computer access is "without authorization" or "exceeds authorized access." The second addresses whether "interruption of service" is a prerequisite for recovery of CFAA damages. The scope of actionable conduct and potential limitations on recovery are addressed below.

Actionable conduct under CFAA can include:

- unauthorized access to Web sites;[148]
- gathering of email addresses;[149]
- diversion of customers and/or harvesting customer lists;[150]
- defective software, including undisclosed disabling code a/k/a "logic bombs;"[151]
- setting of cookies;[152]
- authorized users exceeding scope of authority;[153]
- overbroad subpoenas of ISPs;[154]

---

[146] 18 U.S.C. § 1030(e)(11).

[147] *Id*. § 1030(e)(8).

[148] *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 578 (1st Cir. 2001).

[149] *Am. Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 451 (E.D. Va. 1998).

[150] *YourNetDating, Inc. v. Mitchell*, 88 F. Supp. 2d 870, 870-71 (N.D. Ill. 2000); *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238, 239 (S.D.N.Y. 2000), *aff'd as modified*, 356 F.3d 393, 395 (2d Cir. 2004); *Internet Archive v. Shell*, 505 F. Supp. 2d 755, 765 (D. Colo. 2007).

[151] *Shaw v. Toshiba Am. Info. Sys., Inc.*, 91 F. Supp. 2d 926 (E.D. Tex. 1999); *N. Tex. Preventive Imaging L.L.C. v. Eisenberg*, 1996 WL 1359212, at *7 (C.D. Cal. Aug. 19, 1996).

[152] *In re Intuit Privacy Litig.*, 138 F. Supp. 2d 1272, 1277 (C.D. Cal. 2001); *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 523-24 (S.D.N.Y. 2001); *Chance v. Ave. A, Inc.*, 165 F. Supp. 2d 1153, 1154 (W.D. Wash. 2001); *In re Pharmatrak, Inc. Privacy Litig.*, 220 F. Supp. 2d 4, 14-15 (D. Mass. 2002), *rev'd*, 329 F.3d 9 (1st Cir. 2003).

[153] *United States v. Morris*, 928 F.2d 504 (2d Cir. 1991).

- review of information;[155] and

- Internet advertising.[156]

Recent decisions by two U.S. Courts of Appeals, however, may limit the effectiveness of CFAA as an effective weapon against franchisees, employees, or others who violate the franchisor's policies and other restrictions on use of their computer systems. The critical issue is the meaning of CFAA's prohibition against accessing a computer "without authorization" or in a manner that "exceeds authorized access." Until recently, it seemed beyond dispute that violation of the terms and conditions upon which one has been granted access to a computer is "without authorization" or "exceeds authorized access." On that basis, the Seventh Circuit[157] held that an employee who erased crucial data on his company laptop before turning it in at the end of his employment violated CFAA.[158]

Earlier this year, however, two other federal appeals courts adopted a much narrower interpretation of CFAA. On April 10, 2012, the Ninth Circuit[159]—sitting *en banc*—reversed a three-judge panel's decision that was consistent with the Seventh Circuit view. In an opinion authored by Chief Judge Kozinski, the Ninth Circuit held in *United States v. Nosal* that CFAA provides no remedy against a group of disloyal employees who retrieved confidential information via their company user accounts and transferred it to a competitor.[160] In other words, so long as the defendant was authorized to access the computer in question, the fact that the access was for an unauthorized purpose did not make it "without authorization" or in a manner that "exceeds authorized access."

On July 26, 2012, the Fourth Circuit[161] expressly adopted the rationale of the Ninth Circuit's decision in *Nosal*. Specifically, the Fourth Circuit held that CFAA provides no remedy against a former employee who—before resigning—had downloaded his employer's proprietary information at the behest of a competitor.[162] The Fourth Circuit found that the defendant's use was ***not*** "without authorization" or in a manner that "exceeds authorized access" on the following basis:

> To protect its confidential information and trade secrets, WEC instituted policies that prohibited using the information without

---

[154] *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004).

[155] *United States v. Czubinski*, 106 F.3d 1069, 1078 (1st Cir. 1997).

[156] *I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc.*, 307 F. Supp. 2d 521, 523 (S.D.N.Y. 2004).

[157] The Seventh Circuit has appellate jurisdiction over the U.S. District Courts in Illinois, Indiana, and Wisconsin.

[158] *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418, 419-21 (7th Cir. 2006).

[159] The Ninth Circuit has appellate jurisdiction over the U.S. District Courts in California, Alaska, Arizona, Hawaii, Idaho, Montana, Nevada, Oregon, and Washington.

[160] *United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012).

[161] The Fourth Circuit has appellate jurisdiction over the U.S. District Courts in Virginia, Maryland, North Carolina, South Carolina, and West Virginia.

[162] *WEC Carolina Energy Solutions LLC v. Miller*, ___ F.3d __, 2012 U.S. App. LEXIS 15441 (4th Cir. July 26, 2012).

> authorization or downloading it to a personal computer. These policies did not restrict Miller's authorization to access the information, however.

The fact that CFAA can provide the basis for criminal penalties was among the rationales articulated by the Fourth Circuit for its narrow reading of the statute. The same is true of the Copyright Act, however—which criminalizes copying by both unlicensed users and licensees exceeding the scope of their authorization. The Fourth Circuit also reasoned that employers had other "means to reign in rogue employees"—including claims for misappropriation of trade secrets. But the wrongful conduct at issue in such cases might well have destroyed the trade secret status of the information. The fact that the plaintiff need not establish trade secret protection is among the reasons that CFAA and similar state computer crimes laws can provide such an effective remedy for wrongful use that involves a computer.

Whatever the merits of the recent CFAA decisions by the Fourth and Ninth Circuits, they make one prospect seem likely. Before too long, the Supreme Court may be called upon to resolve conflicting views of the scope of CFAA.

In the interim, another unsettled issue is the proper interpretation of CFAA's provision for the recovery of damages related to "interruption of service." Does it apply only to "any revenue lost, cost incurred, or other consequential damages"? Or must a plaintiff show "interruption of service" to obtain any damages? There is a split of authority on this issue.

Based on the literal language of the statute, many courts have held that the mere cost of investigating and responding to the offense—including the cost of a forensic expert—can be recovered pursuant to 18 U.S.C. § 1030(e)(11). The Fourth Circuit, for example, has observed that CFAA is a "broadly worded provision [that] plainly contemplates consequential damages . . . [including] costs incurred as part of the response to a CFAA violation, including the investigation of an offense."[163] The "loss" recoverable under CFAA, the Fourth Circuit held, thus included "numerous man-hours . . . spent responding" to unauthorized access of a computer including an investigation).[164] A federal district court similarly found a sufficient basis for a default judgment under CFAA in view of allegations of "loss" that included "[c]osts associated with investigating intrusions into a computer network and taking subsequent remedial measures" totaling at least $5,000.[165]

In some cases, federal courts have denied recovery not because the plaintiff failed to allege "interruption of service" but because the alleged damage was not based on a CFAA violation. The U.S. District Court for the Middle District of Tennessee, for example, found no "loss" for purposes of CFAA because the "loss at issue is the misappropriation of [plaintiff]'s

---

[163] *A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 646 (4th Cir. 2009).

[164] *Id.* at 645.

[165] *Barnstormers, Inc. v. Wing Walkers, LLC*, No. EP-10-CV-261-KC, 2011 U.S. Dist. LEXIS 47143, *29-30 (W.D. Tex. May 3, 2011). *See also Jedson Eng'g, Inc. v. Spirit Constr. Servs*., 720 F. Supp. 2d 904, 929 (S.D. Ohio 2010) (CFAA "losses comprise costs incurred in responding to an offense: and restoring the data, program, system or information to its condition prior to the offense" such that a litigant could recover for costs associated with "investigating ways to make the website more secure") (quotation omitted); *SuccessFactors, Inc. v. Softscape, Inc*., 544 F. Supp. 2d 975, 980-81 (N.D. Cal. 2008) (cost of investigating and identifying the CFAA offense, including "many hours of valuable time away from day-to-day responsibilities, causing losses well in excess of $5,000," qualified as costs of responding to an offense).

confidential, trade-secret information, which has damaged [plaintiff]'s business interests."[166] Similarly, the U.S. District Court for the Eastern District of Tennessee concluded in one case that the plaintiff failed to demonstrate loss when it alleged that it "suffered damages as a result of . . . misappropriation of information and proprietary information" and did not allege "that it incurred any costs."[167] In contrast, that same court has since found sufficient for purposes of Rule 12(b)(6) the allegations of a complaint that defendant's actions had "resulted in loss and damage to [plaintiff] in excess of $ 5,000 in value, including . . . the attendant costs of conducting a damage assessment and restoring data to the condition prior to [defendant's] actions."[168] The allegations of "damage" that the court found sufficient included the allegation that defendant's actions had caused plaintiff to "institute remedial measures and restore the computer system to the condition it was in prior to the alleged damage."[169] The court so held considering the "liberal pleading standard and the Court's standard for review of a motion to dismiss."[170]

Last but not least, there are some courts that have held that failure to allege "interruption of service" is an absolute bar to recovery under CFAA.[171]

3. State Computer Crimes Laws

Such statutes typically prohibit "use" of computers "without authority." If the statute does not afford a private right of action, it can be combined with common law trespass. Typical remedies include—in addition to damages—sealing the record, injunctive relief, and costs and attorneys' fees.

The Virginia Computer Crimes Act[172] is typical of enactments in this area. The offenses of the Virginia Computer Crimes Act are keyed to "use" of computers "without authority." "Use" of computers is defined as follows:

A person "*uses*" a computer or computer network when he:

1. Attempts to cause or causes a computer or computer network to perform or to stop performing computer operations;

---

[166] *ReMedPar, Inc. v. AllParts Med., LLC*, 683 F. Supp. 2d 605, 614 (M.D. Tenn. 2010) (concluding and which does not constitute a loss for purposes of CFAA).

[167] *ES&H, Inc. v. Allied Safety Consultants, Inc*., No. 3:08 CV 323, 2009 U.S. Dist. LEXIS 84409, *10 (E.D. Tenn. Sept. 16, 2009).

[168] *Expert Janitorial, LLC v. Williams,* No. 3:09 CV 283, 2010 U.S. Dist. LEXIS 23080, *22-23 (E.D. Tenn. Mar. 12, 2010).

[169] *Id*. at *25.

[170] *Id*. at *23.

[171] *See, e.g., Cenveo Corp. v. CelumSolutions Software GMBH & Co KG*, 504 F. Supp. 2d 574, 581 (D. Minn. 2007) (dismissing CFAA claim based upon improper access to an employer's confidential information because the complaint did not allege an interruption of service, and therefore failed to allege loss); *Spangler, Jennings & Dougherty, P.C. v. Mysilwy*, 2:05-cv-00108-JTM-APR, at *12-13 (N.D. Ind. Mar. 21, 2006) (finding that allegations of downloading of firm information by an attorney who was leaving her employer failed to demonstrate a CFAA because there was no allegation of system impairment, and therefore no loss).

[172] Va. Code § 18.2-152.1 *et seq.*

2. Attempts to cause or causes the withholding or denial of the use of a computer, computer network, computer program, computer data or computer software to another user; or

3. Attempts to cause or causes another person to put false information into a computer.[173]

"Without authority" is defined as follows:

> A person is "*without authority"* when he has no right or permission of the owner to use a computer, or, he uses a computer in a manner exceeding such right or permission.[174]

The specific offenses prohibited by the Virginia Computer Crimes Act—all of which involve "use" of a computer "without authority"—are computer fraud,[175] computer trespass,[176]

---

[173] Va. Code § 18.2-152.2(4) (emphasis in original).

[174] *Id.* (emphasis in original).

[175] "Computer fraud" is defined as follows:

> Any person who uses a computer or computer network without authority and with the intent to:
>
> 1. Obtain property or services by false pretenses;
>
> 2. Embezzle or commit larceny; or
>
> 3. Convert the property of another shall be guilty of the crime of computer fraud. If the value of the property or services obtained is $200 or more, the crime of computer fraud shall be punishable as a Class 5 felony. Where the value of the property or services obtained is less than $200, the crime of computer fraud shall be punishable as a Class 1 misdemeanor.

Id. § 18.2-152.3.

[176] "Computer trespass" is defined as follows:

> Any person who uses a computer or computer network without authority and with the intent to:
>
> 1. Temporarily or permanently remove computer data, computer programs, or computer software from a computer or computer network;
>
> 2. Cause a computer to malfunction regardless of how long the malfunction persists;
>
> 3. Alter or erase any computer data, computer programs, or computer software;
>
> 4. Effect the creation or alteration of a financial instrument or of an electronic transfer of funds;
>
> 5. Cause physical injury to the property of another; or
>
> 6. Make or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs, or computer software residing in, communicated by, or produced by a computer or computer network shall be guilty of the crime of computer trespass, which shall be punishable as a Class 1 misdemeanor. If such act is done maliciously and the value of the property damages is $2,500 or more, the offense shall be punishable as a Class 6 felony.

Id. § 18.2-152.4.

computer invasion of privacy,[177] theft of computer services,[178] and personal trespass by computer.[179]

Persons injured by violations of the Virginia Computer Crimes Act can also recover damages, including lost profits, and the "costs of suit."[180]

It may be possible to prevent competitors and others from learning of the dispute. For example, the Virginia Computer Crimes Act expressly authorizes sealing the record:

> At the request of any party to an action brought pursuant to this section, the court may, in its discretion, conduct all legal proceedings in such a way as to protect the secrecy and security of the computer, computer network, computer data, computer program, and computer software involved ***in order to prevent possible recurrence of the same or a similar act by another person and to protect any trade secrets of any party*** [181] .

Similarly, every federal court "has supervisory power over its own records and files."[182]

---

[177] "Computer invasion of privacy" is defined as follows:

> A. A person is guilty of the crime of computer invasion of privacy when he uses a computer or computer network and intentionally examines without authority any employment, salary, credit or any other financial or personal information relating to any other person. Examination' under this section requires the offender to review the information relating to any other person after the time at which the offender knows or should know that he is without authority to view the information displayed.
>
> B. The crime of computer invasion of privacy shall be punishable as a Class 3 misdemeanor.

Id. § 18.2-152.5.

[178] "Theft of computer services" is defined as:

> Any person who willfully uses a computer or computer network, with intent to obtain computer services without authority, shall be guilty of the crime of theft of computer services, which shall be punishable as a Class 1 misdemeanor."

Id. § 18.2 152.6.

[179] "Personal trespass by computer" is defined as:

> A. A person is guilty of the crime of personal trespass by computer when he uses a computer or computer. network without authority and with the intent to cause physical injury to an individual.
>
> B. If committed maliciously, the crime of personal trespass by computer shall be punishable as a Class 3 felony. If such act be done unlawfully but not maliciously, the crime of personal trespass by computer shall be punishable as a Class 1 misdemeanor.

Id. § 18.2-152.7.

[180] *Id*. § 18.2-152.12.

[181] Va. Code § 18.2-152.12(B) (emphasis supplied); *United Parcel Service, Inc. v. Matuszek*, Case No. 1:97-cv-00744 (E.D. Va. 1997) (hacking to reconstruct competitor's customer list). Mr. Lockerby represented the plaintiff in this case.

[182] *Nixon v. Warner Communications, Inc.*, 435 U.S. 589, 598 (1978).

VII. CONCLUSION

Few if any companies, in franchising or otherwise, would leave their headquarters doors unlocked, much less deposit money in a bank whose vault was not secure. Although trade secrets can be among the most valuable assets of a franchise system, they are all too often left in the equivalent of an unlocked safe. Unlike other forms of intellectual property—for which there are formalities of protection prescribed by federal law—trade secret protection is *ad hoc* and a question of fact under state laws that are not always uniform. Still, there are certain best practices that every franchisor can and should adopt to maintain trade secret protection. In the Internet age, following the best practices set forth herein is more than advisable. It may be essential for survival of the franchise system whose value depends on trade secrets for which franchisees will pay royalties only if they are truly secret.

HEATHER C. PERKINS

Heather Perkins is a partner in the Business Litigation group in the Denver office of Faegre Baker Daniels LLP. She specializes in franchise and distribution litigation, trade secret litigation and counseling, and litigating complex commercial matters. Her trade secret and franchise litigation practices have taken her to court many times either seeking or defending against temporary restraining orders and requests for preliminary injunctive relief. Heather has represented manufacturers, franchisors, dealers, and distributors in federal and state proceedings, arbitrations, and mediations around the country.

Heather frequently speaks and writes on franchising and trade secret matters. Her recent presentations include *Availability and Provability of Damages in Franchise Litigation* Co-Presenter, International Franchise Association (2010) and *The 5 Most Frequently Filed Lawsuits Against Franchisors — And How to Avoid Them*, Co-Presenter, International Franchise Association Legal Symposium (2008). She recently co-authored *Franchisor Liability for Acts of the Franchise,* Franchise Law Journal, Winter 2010, was a contributing author to *The Secrets to Winning Trade Secret Cases*, Thomson West (2nd Ed. 2010-11), and was a contributing author to the upcoming *Covenants Against Competition in Franchise Agreements, Third Edition.*

Heather graduated with honors from the University of Colorado School of Law in 1998. She graduated with honors from the University Colorado School of Business with a bachelors of science degree with emphases in accounting and finance in 1993. Between college and law school, she practiced as a Certified Public Accountant in Colorado and Chicago. Immediately after graduating from law school, she served for two years as a law clerk to a United States District Judge in Denver, Colorado.

JAMES P. MITTENTHAL

James P. Mittenthal is Vice President, Consulting Services for Epiq Systems, resident in its New York office. Jim has assisted national law firms and law departments for more than 26 years on a wide range of technology initiatives and general management issues. His practice specialties include strategic technology planning, information life cycle management, litigation support and related system selection, and implementation in both legal practice and administration. He serves in technology-based cases as a testifying or consulting expert, as a corporate witness in product liability matters, and undertakes technology-based investigations and remediation assignments. Jim also manages the discovery and production lifecycle of enterprise and legacy data, particularly in the health and financial services sectors. Prior to joining Epiq, Jim developed a suite of commercial software and custom applications for complex litigation management, used by law firms, large corporations, and government entities. He later worked at Price Waterhouse and Hildebrandt Baker Robbins through its acquisition by Thomson Reuters. He attended the University of Michigan and obtained his J.D. from Boston University. Jim's most recent publication, "Managing Enterprise Discovery in Pharmaceutical and Medical Device Litigation," appeared in the March/April 2012 edition of *Pharma* Magazine.

MICHAEL J. LOCKERBY

Michael J. Lockerby is a partner with the law firm of Foley & Lardner LLP and one of the co-chairs of the firm's national Distribution & Franchise Practice Group and of the Washington, D.C. office Litigation Department. He is also a member of the firm's Privacy, Security & Information Management and its Trade Secret Noncompete Practice Groups.

For the past 28 years as a trial lawyer, Mr. Lockerby has been on the cutting edge of the intellectual property, antitrust, business tort, and franchise law issues that face all manufacturers and other suppliers whose products are sold through independent dealers, distributors, and franchisees. He has appeared throughout the country in state and federal trial courts and before arbitrators and other ADR providers. His litigation and counseling practice includes trade secret protection and "computer crimes," and he is frequently in court on motions for preliminary injunctive relief and temporary restraining orders.

Mr. Lockerby has been a prolific author and speaker at the ABA Forum on Franchising, the International Franchise Association, and the ABA Section of Antitrust Law, among other organizations. On behalf of the ABA Section of Antitrust Law, he previously chaired the Distribution & Franchise Committee. On behalf of the Forum on Franchising, Mr. Lockerby has previously served on the Editorial Board of the *Franchise Law Journal* and as Editor-in-Chief of *The Trade Secret Handbook: Protecting Your Franchise System's Competitive Advantage*.

Mr. Lockerby received a B.A. from the University of North Carolina at Chapel Hill and a J.D. from the University of Virginia. He previously worked as a legislative assistant for the late Senator John Heinz (R-Pennsylvania).