American Bar Association
41st Annual Forum on Franchising

CYBERSECURITY: PUTTING THE TOOTHPASTE BACK IN THE TUBE – BEST PRACTICES FOR RESPONDING TO A SECURITY BREACH

Jason Adler
Cellairis Franchise, Inc.
Atlanta, Georgia

Eleanor Vaida Gerhards
Fox Rothschild LLP
Warrington, Pennsylvania

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

October 10 – 12, 2018
Nashville, Tennessee

TABLE OF CONTENTS

I. INTRODUCTION

When most people hear that a franchise system suffered a "security breach," the immediate assumption is that the franchisor or a franchisee was a victim of one of the almost daily data breaches involving the theft of third-party data, such as customer personally identifiable information or credit card data. Seasoned franchise attorneys understand, however, that breaches involving the franchisor's own trade secrets—such as its operations manuals, policies, recipes and formulas, or business plans—can threaten the value or even the very survival of the franchise system. Regardless of whether a security breach involves the franchisor's own trade secrets, such as its operations manuals, policies, recipes and formulas, or business plans, or third party data such as customer or franchisee information, the resultant business and legal issues are similar. Failure to act quickly and appropriately may mean that trade secrets and confidential information lose their protected status by ending up in the public domain. The result can be a tremendous loss of value to the franchisor and its franchisees and can expose the franchisor to claims by shareholders, franchisees, and/or customers. What is the allocation of loss between franchisor and franchisee? This panel will address best practices for salvaging the value of compromised trade secrets and third party data, and—where necessary—litigating against the wrongdoers. In this regard, many of the potential causes of action against the wrongdoers may be the same regardless of whether the security breach involved the franchisor's trade secrets or third party data. The viability of certain claims, however, may depend upon whether the breach caused any trade secrets—those of the franchisor, those of a franchisee, or those of a third party—to lose their status as such. Fortunately, the viability of the so-called "computer crimes" causes of action discussed in this paper does not depend upon whether the information at issue is a trade secret (or was before the breach).

II. WHAT IS A TRADE SECRET?

An attorney representing a franchise system should clearly understand what information constitutes a protectable trade secret. If a franchise system does not have a firm understanding of its own trade secrets, then it may not know to take the necessary precautions to preserve their secrecy and ensure protection under the law in the event of a breach. Additionally, in today's age of the Internet and social media, information can disseminate at exceptionally fast rates. As a result, the measures taken by a franchise brand when there is a breach could be the difference between the protection and enforceability of a trade secret and the loss of trade secret protection because the information has become too public. The loss of trade secret protection status for something as valuable as a brand's "secret sauce" could lead to a loss of potential new franchisees as well as subsequent litigation by current franchisees.

A. Trade Secret Background

"Trade secret law serves to protect 'standards of commercial morality' and 'encourage [ ] invention and innovation' while maintaining 'the public interest in having free and open competition in the manufacture and sale of unpatented goods.'"[1] Determining what constitutes a trade secret requires a factual examination of the particular type of information sought to be protected. The

---

[1] *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262, 1263 (7th Cir. 1995) (quoting MELVIN F. JAGER, TRADE SECRETS LAW § IL.03 at IL–12 (Clark Boardman Callaghan, rev. ed. 1994)).

Uniform Trade Secrets Act (the "UTSA")—enacted in 47 states[2] plus the District of Columbia, Puerto Rico, and the U.S. Virgin Islands[3]—defines a "trade secret" as:

> [I]nformation, including a formula, pattern, compilation, program, device, method, technique, or process, that:
>
> > (i) Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and
> >
> > (ii) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[4]

The franchisor has the burden of establishing that its trade secrets have been "the subject of efforts that are reasonable under the circumstances to maintain [their] secrecy."[5] To determine the reasonableness of the franchisor's security measures, courts consider:

1. "the existence or absence of an express agreement restricting disclosure;"
2. "the nature and extent of security precautions taken by the [franchisor] to prevent acquisition of the information by unauthorized third parties;"
3. "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"
4. "the degree to which the information has been placed in the public domain or rendered 'readily ascertainable.'"[6]

There are numerous types of trade secrets that are associated with franchise systems. The dissemination of any of this information could have major consequences to the franchisor. In the words of a North Carolina Court of Appeals decision:

> misappropriation of a trade secret is an injury of "such continuous and frequent recurrence that no reasonable redress can be had in a court of law." The very nature of a trade secret mandates that misappropriation will have significant and continuous long-term

---

[2] The three states that have not enacted some version of the UTSA are Massachusetts, New York, and North Carolina.

[3] Arkansas, California, Connecticut, Indiana, Louisiana, Rhode Island, and Washington adopted the 1979 version of the UTSA. The remaining 40 states and the District of Columbia, Puerto Rico, and the U.S. Virgin Islands adopted the 1985 version.

[4] UTSA § 1(4)(1985). As discussed herein with respect to the 2016 Defend Trade Secrets Act, the federal definition is substantively similar.

[5] *Id.*

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

> effects. The party wronged may forever lose its competitive business advantage or, at the least, a significant portion of its market share.[7]

B. Potential Loss of Confidentiality by Internet Posting

Regardless of whether the cybersecurity breach involves trade secrets or third party data, posting on the Internet of whatever was "hacked" may destroy the confidentiality of the information, including its protectability as a trade secret. Two leading cases in which posting of trade secrets on the Internet caused the "franchisor" to lose trade secret protection involved the licensing affiliate of the Church of Scientology: the 1995 decision of the U.S. District Court for the Northern District of California in "*Netcom*"[8] and the 1995 decision of the U.S. District Court for the Eastern District of Virginia in "*Lerma*."[9]

These cases are of particular importance to franchisors for three reasons. First, the Church of Scientology operates very much like a franchise, deriving substantial licensing revenues from the trade secrets at issue in *Netcom* and *Lerma*. These trade secrets include 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." 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.

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."[10] 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

---

[7] *Merck & Co. v. Lyon*, 941 F. Supp. 1443, 1455 (M.D.N.C. 1996) (quoting *Barr–Mullin, Inc. v. Browning*, 108 N.C. App. 590, 597, 424 S.E.2d 226, 230 (1993)).

[8] *Religious Technology Center v. Netcom On-Line Communication Services*, 923 F. Supp. 1231 (N.D. Cal. 1995).

[9] *Religious Technology Center v. Lerma*, 908 F. Supp. 1362 (E.D. Va. 1995).

[10] *Netcom*, 923 F. Supp. at 1256 (footnotes omitted).

> Internet information cannot be liable for misappropriation because there is no misconduct involved in interacting with the Internet.[11]

Notwithstanding earlier decisions like *Netcom* and *Lerma*, more recent cases hold that posting trade secrets on the Internet does not automatically result in their loss if the publication is "sufficiently obscure or transient or otherwise limited so that it does not become generally known to ... potential competitors."[12] Such authority is even more reason to pursue preliminary injunctive relief and other remedies promptly.

C. Common Protectable Trade Secrets in Franchising

Examples of franchise system trade secrets that courts have found to be protectable include: (1) strategic information; (2) computer software systems; (3) customer information; (4) recipes and formulas; (5) methods of operation, processes, and techniques; (6) operations manuals; (7) prospective franchisee information; (8) line extensions and launch dates; and (9) supply agreements.

1. Strategic Information

In *Camp Creek Hospitality Inns, Inc. v. Sheraton Franchise Corporation*,[13] strategic information was deemed a protectable trade secret. The franchisee claimed that the manager of a nearby corporately operated hotel, who had been responsible for the brand's reservation system, "improperly came into possession of information concerning the franchisee's occupancy levels, average daily rates, discounting policies, rate levels, long term contracts, marketing plans, and operating expenses."[14] Evidence showed that the manager "used this information to propose the Inn's [franchise's] ejection from the Sheraton system and that he may have used it to compete against the Inn for customers."[15]

The Eleventh Circuit concluded that the franchisee "provided evidence upon which a reasonable jury could find that the information in this case meets Georgia's statutory definition of a trade secret."[16] In doing so, the court relied on the franchisee's expert testimony, which suggested "that this information is closely guarded in the hotel industry, that a competitor could not easily derive the information through other means, and that a competitor could make use of

---

[11] *Lerma*, 908 F. Supp. at 1368.

[12] *DVD Copy Control Ass'n v. Bunner*, 116 Cal. App. 4th 241, 10 Cal. Rptr. 3d 185 (2004).

[13] 139 F.3d 1396 (11th Cir. 1998).

[14] *Id.* at 1410.

[15] *Id.*

[16] *Id.* at 1411. The Eleventh Circuit succinctly stated "[t]o support a claim for misappropriation of trade secrets, Camp Creek must show that (1) it had a trade secret and (2) the opposing party misappropriated the trade secret." *Id.* at 1410 (citing generally, *DeGiorgio v. Megabyte Int'l, Inc.*, 266 Ga. 539, 468 S.E.2d 367 (1996) (applying GA. CODE §§ 10–1–761, 763)). The State of Georgia, where the franchised unit was located and whose law applied to this claim, "defines trade secrets broadly to include non-technical and financial data that derives economic value from not being generally known and is the subject of reasonable efforts to maintain its secrecy." *Id.* at 1410 (citing generally, *DeGiorgio*, 266 Ga. 539, 468 S.E.2d 367 (1996); GA. CODE § 10–1–761(4)).

such information to the detriment of the owner." Therefore, this information had economic value.[17] With respect to the secrecy prong of the trade secret definition, the court concluded that "although Camp Creek did provide the information to Sheraton, it provided that information pursuant to the Reservation Agreement and on the apparently mutual understanding that it would be kept confidential."[18]

Like the franchisor in *Camp Creek*, the franchisor of the Mirko system at issue in *Bans Pasta, LLC v. Mirko Franchising, LLC*[19] "developed and implemented a 'valuable, unique, and reputable' franchise model, wherein . . . [it] 'licenses to franchisees the rights to use Mirko's brand and confidential information and trade secrets.'"[20] The franchisor provided the franchisee "'a variety of confidential and proprietary information concerning Mirko's brand, including standard specifications, procedures, and methods for setting up and operating'" a Mirko restaurant."[21]

The franchisee signed a franchise agreement and the two owners signed a confidentiality agreement whereby "they agreed, among other things, not to disclose trade secrets or confidential information as defined in the [Franchise] Agreement, and not to 'utilize any Confidential Information or Trade Secrets other than for the benefit of [Bans].'"[22] After the franchised location's opening, a dispute arose between the parties. Although the franchisee claimed that the franchise agreement had been constructively terminated, for a period of almost five months, the franchisee "continued to operate the Restaurant as a Mirko franchise, including displaying Mirko's proprietary signage and selling foods and beverages from Mirko's proprietary recipes and specifications."[23] Ultimately, the franchisee ceased franchise operations and began running another restaurant from the same location.[24] The franchisor formally terminated the franchise agreement.[25]

The franchisee filed a lawsuit relating to the parties' failed relationship, and the franchisor filed a five-count counterclaim, including a trade secret misappropriation claim.[26] The court quoted *Camp Creek* and used the same language for determining a claim for misappropriation of trade secrets under Georgia law, the choice of law provided for in the Franchise Agreement. The

---

[17] *Id.* at 1411.

[18] Id. at 1411.

[19] Bus Franchise Guide (CCH) ¶ 15,503 (W.D. Va. May 23, 2014).

[20] *Id.* at 1.

[21] *Id.*

[22] *Id.* at 2.

[23] *Id.* at 3.

[24] *Id.*

[25] *Id.*

[26] *Id.* at 2. The five counts in the counterclaim were: (i) breach of contract against the franchisee seeking damages of not less than $235,760.84; (ii) breach of the guaranty; (iii) breach of contract claims against the franchisee relating to the confidentiality provisions; (iv) breach of contract claims against the owners of the franchisee relating to the confidentiality provisions; and (v) claims against the franchisee and its owners for misappropriation of trade secrets under the Georgia Trade Secrets Act. *Id.*

district court determined that the standard specifications, methods, and procedures were "adequately pled" by the franchisor to "describe its trade secrets."[27] The district court also ruled that "[t]he statute expressly defines 'improper means' as including 'breach . . . of a confidential relationship or other duty to maintain secrecy or limit use.'"[28] Thus allowing the franchisor's trade secret misappropriation claim to survive the motion to dismiss.[29]

2. Computer Software Systems

The use of technology is a critical component of most franchise systems. In *Rivendell Forest Products, Ltd. v. Georgia-Pacific Corporation*, which did not involve franchising, the court determined that the computer system in question was a protectable trade secret.[30] The plaintiff sued both the defendant entity and its former employee for trade secret misappropriation relating to plaintiff's computer software system that allowed plaintiff to manage its operations and:

> enabled Rivendell employees to give immediate answers to customers' questions and phone inquiries as to prices, quantities, places, and delivery time as to various lumber sizes and types without any computations which required a delay and a call back to the customer. It asserted that at the pertinent time no other wholesaler could provide such service and management, and this gave Rivendell a large advantage over its competitors including G.P. [defendant].[31]

The Tenth Circuit held:

> that the doctrine has been established that a trade secret can include a system where the elements are in the public domain, but there has been accomplished an effective, successful and valuable integration of the public domain elements and the trade secret gave the claimant a competitive advantage which is protected from misappropriation.[32]

---

[27] *Id.* at 5 (citing *Atlantic Fiberglass USA, LLC v. KPI, Co., Ltd.*, 911 F. Supp. 2d 1247, 1259 (N.D. Ga. 2012) (denying motion to dismiss a misappropriation of trade secrets claim where the claimant alleged that "it developed trade secrets in the form of 'technical data, methodologies, product plans, and other trade secret information' related to its 'special order fiberglass product.'")).

[28] *Id.* at 5-6 (quoting GA. CODE § 10-1-761(1); citing *Camp Creek Hospitality Inns, Inc.*, 139 F.3d at 1412 ("the GTSA includes the diversion of information acquired under legitimate circumstances within its definitions of misappropriation")).

[29] *Id.* at 6.

[30] 26 F.3d 1042, 1046 (10th Cir. 1994).

[31] *Id.* at 1043.

[32] *Id.* at 1046.

The court's finding of trade secret protection in *Rivendell* has direct application to many franchise systems—particularly those in which the franchisor uses or provides a reservation system, scheduling software, or some other computer system in franchise operations.

3. Customer Information

Customer information, which may be considered strategic information in its own right, has specifically been deemed to be a protectable trade secret. In *American Express Financial Advisors, Inc. v. Yantis,*[33] Mr. Yantis was a franchisee of a system that provided financial advice to its customers. Approximately five years after becoming a franchisee, Mr. Yantis began working for a competitor.[34] The franchisor filed both a five count complaint and a motion for a preliminary injunction.[35] Count Two of the complaint alleged misappropriation of the franchisor's trade secrets.[36]

The franchise agreement contained the following trade secret provision:

> Independent Advisor [Mr. Yantis] has had and/ or may have access to AEFA trade secrets and confidential information that Independent Advisor agrees has great value to AEFA. Independent Advisor agrees that because of such access, Independent Advisor is in a position of trust and confidence with respect to this information. To protect client confidentiality, AEFA goodwill, trade secrets, and other proprietary and confidential business information, Independent Advisor agrees to not, during the term of this Agreement or thereafter . . . communicate, divulge, or use for himself or herself except pursuant to the System, or for the benefit of any other person, partnership, association, or corporation any confidential information, or trade secrets, including, without limitation, Client names, addresses and data and know-how concerning the methods of operation of the System and the business franchised hereunder which may be communicated to Independent Advisor or of which Independent Advisor may be apprised by virtue of Independent Advisor's operation under the terms of this Agreement. Independent Advisor also shall not reveal any information about potential clients to whom a presentation has been made by any Independent Advisor who might reasonably be expected to do business with AEFA. . . . Independent Advisor agrees that, without limitation, Client names, addresses, data and other personal and financial information recorded in Client records are confidential. Confidential information includes compilations and lists of such Client information even if of otherwise public

---

[33] 358 F. Supp. 2d 818 (N.D. Iowa 2005).

[34] *Id.* at 824.

[35] *Id.* at 824-25.

[36] *Id.* at 824. The four other counts within the complaint were (i) breach of contract; (ii) conversion of client files; (iii) unfair competition; and (iv) request for injunctive relief. *Id.* at 824.

> information if such compilations or lists were the result of substantial effort, time and/ or money expended pursuant to the System. Independent Advisor further agrees to use this confidential information only in furtherance of this Agreement or in accordance with the Manuals and for no other purpose.[37]

The franchise agreement that Mr. Yantis signed also contained the following language about the use of any such trade secrets after termination:

> • Independent Advisor agrees to immediately and permanently cease to use, in any manner whatsoever, any confidential methods, procedures, and techniques associated with the System....
>
> * * * * * *
>
> • Independent Advisor agrees to immediately deliver to AEFA the Manuals and all other original records, including most recent financial plans and recommendations, computer databases and files, correspondence, and instructions containing confidential information relating to the System (and any copies thereof, including electronic or computer generated copies, even if such copies were made in violation of this Agreement), all of which are acknowledged to be the property of AEFA....[38]

The franchisor alleged that Mr. Yantis kept "client names, addresses, and data, including suitability information, investments and investment history, financial plans, financial goal information, prospective client names, addresses, and data, and know-how concerning the methods of operation, client lists and other financial information."[39] The court determined that

---

[37] *Id.* at 821-22.

[38] *Id.* at 822.

[39] *Id.* at 830.

customer information was a protectable trade secret[40] because "the information is a compilation of information about AEFA's clients and their financial histories and future goals."[41]

The court also determined that the franchisor took reasonable measures to protect the secrecy of the information. These measures included requiring the franchisee to execute a franchise agreement that set forth the franchisee's obligations with respect to disclosure obligations of various types of information. The franchise agreement also contained a detailed section defining the meaning of the term "confidential information."[42] In addition to obligating Mr. Yantis as franchisee to maintain secrecy, the franchise agreement also required the franchisee to have any staff who would come into contact with any such confidential information to sign confidentiality agreements.[43] Finally, with respect to the use of any such information, the franchisee agreed to:

> not, during the term of this Agreement or thereafter, except as permitted under Section 14 regarding transfers of the Independent Financial Advisor Business, communicate, divulge, or use for himself . . . except pursuant to the System, or for the benefit of any other person, partnership, association, or corporation any confidential information, or trade secrets, including, without limitation, Client names, addresses and data and know-how concerning the methods of operation of the System and the business franchised under which may be communicated to

---

[40] *Id.* In reaching this conclusion, the district court first determined that "[t]rade secrets are protected under the Iowa Uniform Trade Secrets Act, Iowa Code Chapter 550...." *Id.* The Iowa statute defines a trade secret as "'information, including but not limited to a formula, pattern, compilation, program, device, method, technique or process....'" *Id.* at 830-31 (quoting IOWA CODE § 550.2(4). The court then turned its attention to whether any of the information the franchisor wanted to protect was, in fact, a trade secret. *Id.* The Iowa Supreme Court explained the following about trade secret protection:

> Under the plain language of [Iowa Code § 550.2(4)], "trade secret" is defined as "information" and eight examples of this term are provided. Although these examples cover items normally associated with the production of goods, "trade secrets" are not limited to the listed examples....
>
> One commentator explains: Trade secrets can range from customer information to financial information about manufacturing processes to the composition of products. There is virtually no category of information that cannot, as long as the information is protected from disclosure to the public, constitute a trade secret.
>
> We believe that a broad range of business data and facts which, if kept secret, provide the holder with an economic advantage over competitors or others, qualify as trade secrets.

Id. at 831 (citing *US W. Commc'ns, Inc. v. Office of Consumer Advocate*, 498 N.W.2d 711, 714 (Iowa 1993) (quoting *Econ. Roofing & Insulating v. Zumaris*, 538 N.W.2d 641, 646–47 (Iowa 1995)).

[41] *Id.* at 831 (citing *Econ. Roofing*, 538 N.W.2d at 647 (recognizing that trade secrets include customer information)).

[42] *Id.* Despite having a one year non-competition provision, the franchise agreement imposed no time limitation on post-termination use of trade secrets obtained from the franchise system. *Id.*

[43] *Id.*

> Independent Advisor or of which Independent Advisor may be apprised by virtue of Independent Advisor's operation under the terms of this Agreement....[44]

As a result of the language in the franchise agreement, the requirement to maintain secrecy and confidentiality, and the state statutory definition of trade secrets, the court determined that the franchisor "has shown a likelihood of success on the merits of its claim that Yantis has acted in violation of the Trade Secrets Act."[45]

4. Recipes and Formulas

Many systems pride themselves on having the "secret sauce" to attract franchisees and customers. Perhaps one of the most recognizable trade secrets in the world is the formula for Coca-Cola. In *Coca-Cola Bottling Company of Shreveport, Inc. v. Coca-Cola Company*, the District Court of Delaware declared (as many other courts have done before) that the formula for Coke is a trade secret.[46] Most of the ingredients that make up the syrup for Coke are public. The "ingredient that gives Coca-Cola its distinctive taste is a secret combination of flavoring oils and ingredients known as 'Merchandise 7X.'"[47] As evidence of the measures taken to protect this trade secret, Coca-Cola Company keeps the formula in a security vault, which "can only be opened upon a resolution from the Company's Board of Directors."[48] Additionally, only two people within the company "know the formula at any one time, and that only those persons may oversee the actual preparation of Merchandise 7X."[49] The company's affidavit further described how the secret formulas are "highly valued assets of the Company and have never been disclosed to persons outside the Company."[50] The court concluded "it is beyond dispute that . . . the Company possesses trade secrets which have been carefully safeguarded and which are extremely valuable."[51]

Although the Coca-Cola formula is known as one of the most protected trade secrets, another well-known formula in franchising—Kentucky Fried Chicken's Original Recipe Fried Chicken's special blend of spices—is protected as a trade secret because it "is prepared by a special cooking process featuring the use of a '"secret recipe"' seasoning known as 'KFC

---

[44] *Id.* at 832.

[45] *Id.* at 833.

[46] 107 F.R.D. 288 (D. Del. 1985).

[47] *Id.* at 289. Coca-Cola Company submitted an affidavit in support of its contention that the formula was in fact a trade secret. *Id.* at 294.

[48] *Id.*

[49] *Id.* In further support of the measures of secrecy and protection taken, the identity of the two people is not disclosed, and they are not permitted to fly together. *Id.*

[50] *Id.* The affidavit explains as an example, that at the time of this case, the company did not expand into of India, which had a market of over 550 million people, because the government would have required the company to disclose the formula. *Id.*

[51] *Id.*

Seasoning."'[52] In litigation brought by KFC against seasoning suppliers, the court concluded that the KFC Seasoning was a trade secret and "constitutes the franchise itself."[53] "To protect the secrecy of the composition of KFC Seasoning, KFC has designed a blending system for making the seasoning"[54] whereby the KFC Seasoning has been separated into two parts. Each part is made by a different company, and "[n]either company has knowledge of the complete formulation" nor of the other company's role in the production of the KFC Seasoning.[55] "Both companies have entered into secrecy agreements with KFC, binding them to maintain the confidentiality of that portion of the KFC Seasoning formula to which each is privy."[56]

In contrast, in *Hutchison v. KFC Corp*oration, the district court held that the plaintiffs' process for cutting, skinning, marinating, dipping, breading, and frying chicken was obvious to those in the business of preparing and selling skinless fried chicken.[57] The basic steps themselves were generally known or readily ascertainable by others and therefore could not qualify as a trade secret. Similarly, in *Sioux Falls Pizza Company v. Little Caesar Enterprises*,[58] the court found that Little Caesar had failed to demonstrate that information comprising its "Hot-N-Ready" system was not "generally known" to the public and was otherwise not protectable as a trade secret. One basis for the court's decision was evidence that other pizza restaurants used similar methods for preparing pizza. The court also found that Little Caesar had not demonstrated reasonable efforts under the circumstances to maintain the secrecy of the Hot-N-Ready system—in part because the confidentiality agreements signed by franchisees did not extend to all of the franchisees' employees.

5. Methods of Operation, Processes, and Techniques

In addition to recipes, a franchise system's methods of operation, processes, and techniques are protectable trade secrets. In *Tan-Line Studios, Inc. v. Bradley*, the plaintiff-franchisor developed a sun tanning franchise. The defendants were various individuals who opened and operated competing tanning salons.[59] The franchisor hired one of the defendants to help prospective franchisees obtain financing. While serving in this role, he received various types of financial information, visited and observed franchised locations, and learned about the "methods of employee recruitment and training, studio layout, cash control, advertising,

---

[52] *KFC Corp. v. Marion-Kay Co., Inc.*, 620 F. Supp. 1160, 1163 (S.D. Ind. 1985).

[53] *Id.* at 1172. *See also Krehl v. Baskin-Robbins Ice Cream Co.*, No. CV 76-1797-DWW, 1979 WL 1662 , at *2 (C.D. Cal. August 7, 1979), *aff'd*, 664 F.2d 1348 (9th Cir. 1982) ("The formulae and processes for manufacturing Baskin-Robbins ice cream products are highly guarded secrets, divulged only to Baskin-Robbins licensed area franchisers who are bound to maintain their confidentiality").

[54] *Id.* at 1163.

[55] *Id.*

[56] *Id.*

[57] 883 F. Supp. 517, 521 (D. Nev. 1993).

[58] 858 F. Supp. 2d 1053 (D.S.D. 2012).

[59] No. CIV.A. 84-5925, 1986 WL 3764, * 4-5 (E.D. Pa. March 25, 1986), *aff'd sub nom. Paul v. Tanning, Health & Fitness Equip. Co.*, 808 F.2d 1517 (3d Cir. 1986), and *aff'd sub nom. Tan-Line Studios, Inc. v. Paul*, 808 F.2d 1518 (3d Cir. 1986).

accounting, marketing, promotion and site selection."[60] The court found that this individual "intentionally misrepresented to Tan-Line that it was his purpose to assist prospective Tan-Line franchisees when in fact he intended to obtain trade secrets and confidential data from Tan-Line for the purpose of competing with Tan-Line."[61]

The court rejected the defendants' argument that the information was not a trade secret and found that the method of business was developed "[t]hrough trial and error, research, and experience gained in the operation of their tanning studios. . . ."[62] The court held that the method of doing business was not known throughout the industry and:

> it includes Tan-Line's methods of employee recruitment and training, studio layout, cash control, advertising, accounting, marketing, promotion, and site selection, among others. Tan-Line's particular method of business also incorporates knowledge and information gained concerning the success and value of different approaches to the various aspects of the indoor sun tanning business.[63]

In rejecting the defendants' assertions and finding that the method of doing business was a trade secret, the court ruled that "[p]erhaps the best evidence supporting my holding . . . is the fact that franchisees are willing to purchase the rights to use and learn the methodology."[64]

The case of *Snelling & Snelling, Inc. v. Armel, Inc.* is a second example of the protection of trade secrets for franchise system "procedures, techniques, methods of operation, training manuals and instructional guides relating to employment office management and supervision. . . ."[65] Snelling & Snelling franchised an employment agency system, with over 500 units throughout

---

[60] *Id.* at *2.

[61] *Id.* at *4. The district court also found that the remaining defendants "knew or should have known that Mr. Bradley had obtained trade secrets and confidential data from Tan-Line and was using this information to Tan-Line's detriment without Tan-Line's permission." *Id.*

[62] *Id.* at *7. The defendants argued that "the information amounted to general knowledge available to anyone who would take the trouble to look for it, and that the information at most constitutes general secrets of the trade rather than the particular secrets of Tan-Line." Id.

[63] *Id.* The defendants also challenged the fact that the plaintiff-franchisor did not specifically identify the specific trade secrets that comprised the method of doing business. However, the court rejected that challenge and held that "Tan-Line's entire methodology for conducting a tanning studio constitutes a trade secret." *Id.*

[64] *Id.* The court continued by pointing out that the former employee defendant himself thought that the information was a "trade secret because he prepared a contract under which he would issue Tan-Line franchises and remunerate Tan-Line at reduced rates." *Id.* Additionally, if the former employee did not think the method of doing business was a trade secret, then he "would not have needed to penetrate the corporate structure of Tan-Line." *Id.* at *8.

[65] 360 F. Supp. 1319, 1321 (W.D. La. 1973).

the country at the time of the civil action.[66] The defendant was a franchisee of the system that opened a competing employment agency business.[67] The court found that plaintiff-franchisor:

> [t]hrough the substantial expenditure of time, effort and money, and as a result of the studies and surveys made by it over the past twenty years, plaintiff has compiled and developed procedures, techniques, methods of operation, training manuals and instructional guides relating to employment office management and supervision, hiring, training and supervision of employees, certain forms, and other methods, all of which are designed to and do give the Snelling & Snelling franchisee a competitive advantage over other agencies not members of the Snelling & Snelling System.[68]

The detailed process, methods of operation, techniques, and other aspects of the business developed by plaintiff-franchisor provided franchisees a competitive edge over other similar businesses, and this information was treated as confidential.[69] This confidential treatment was carried out in a similar manner to that in the other cases discussed within this section and in general conformity with most franchise agreements in existence today. The defendant signed a franchise agreement, and the individual owners of the franchise agreed to be personally bound by the agreement.[70] Specifically, the defendant and its owners "agreed that the methods and techniques employed by Snelling were of considerable value and that the operations manuals and information contained therein were confidential. . . ."[71] The court found that the new business operated by defendant "utilized the information, techniques, methods of operation and procedures disclosed to defendants in confidence at the same location. . . ."[72] The *Snelling & Snelling* case clearly establishes that such methods of operation, techniques, and procedures, which are at the core of franchising, are protectable trade secrets.

SmokEnders, Inc. v. Smoke No More, Inc. provides a third example of a case in which trade secret protection extended to not only the method of doing business but also the manual used for those operations. The court held that they were both protectable trade secrets.[73] The plaintiff-franchisor was in the business of teaching its customers to stop smoking by using a commercial program that was developed by its founder through extensive research and trial and error in her own quest to stop smoking (which was achieved).[74] This work resulted in the creation

---

[66] *Id.* at 1320.

[67] *Id.* at 1320-21.

[68] *Id.* at 1320.

[69] *Id.*

[70] *Id.*

[71] *Id.*

[72] *Id.* at 1321.

[73] No. 73-1637, 1974 WL 20234 (S.D. Fla. Oct. 21, 1974).

[74] *Id.* at *2.

of a manual.[75] The court found that the "trade secret resides in the composite program as it is arranged for step-by-step delivery to the attendees"[76] and it specifically held that:

> [t]he SE program is a trade secret in that it is (1) the product of many hours of labor, (2) of commercial value to competitors, (3) could only be prepared by competitors at great expense, (4) has been kept secret by agreement and complexity of the program, and (5) is novel.[77]

The court further held that a trade secret could be found "in a combination of characteristics and components, each of which, by itself, is in the public domain, but the unified process design and operation of which in unique combination affords a competitive advantage and is [a] protectable trade secret."[78] The court then determined that the plaintiff-franchisor had a right to keep the methods, processes, and work it did to itself if plaintiff-franchisor either did the work or paid for it. The "fact that others might do similar work, if they might, does not authorize them to confiscate it."[79] The court ultimately held that the defendants misappropriated plaintiff's trade secrets and concluded:

> Where one invests substantial time, thought and money in collecting and testing data and creating and perfecting forms and processes and techniques that provide the substance and detail of a commercial program, that program will be protected from misappropriation if it is provided with qualified secrecy and is not publicly available in its specific form.[80]

6. Operations Manuals

Franchise operations manuals have also been afforded trade secret status. As seen in the *SmokEnders* case discussed above, the operations manual played an integral role within the franchise system.[81] When the plaintiff-franchisor trained the defendant's individual owners, "the manual was extensively revised to include empirical data accumulated as a result of four (4) years

---

[75] *Id.* The manual "contain[ed] [the founder's] smoke cessation concept and techniques and is specifically structured for communicating them to smokers in a classroom lecture situation." By 1972, the time when the issues with defendant started, the manual and the techniques for using the manual as a didactic tool represented nineteen years of Rogers' experience, research, and development. *Id.*

[76] *Id.* at *3.

[77] *Id.* at *3.

[78] *Id.* at *11 (citing *Water Servs., Inc. v. Tesco Chemicals, Inc.*, 410 F.2d 163, 173 (5th Cir. 1969)).

[79] *Id.* (citing *Bd. of Trade of City of Chicago v. Christie Grain & Stock Co.*, 198 U.S. 236 (1905); *Clark v. Bunker*, 453 F.2d 1006, 1009-10, (9th Cir. 1972)).

[80] *Id.* at *12 (citing *Clark*, 453 F.2d at 1010).

[81] *Id.* at *3.

of conducting business."[82] The franchise program's "moderators" (the term used to identify the system operators who taught the classes) were to "follow the SE [franchisor] manual with very little departure from the text material and impose the step-by-step regimentation contained therein on the seminar attendees."[83]

The court found that the franchisor took "elaborate precautions to maintain the confidentiality of the substance of its program and to maintain the confidentiality of its manual."[84] The franchisor required "attendees of the program to agree in writing before they are admitted to the program that they will not appropriate nor disclose any portion of the SE program."[85] The length of the program was too long for anyone to memorize it.[86] Furthermore, the moderators were loaned a copy of the manual only after completing the training program.[87] Additionally, after each nine-week session, the moderator must return the manual until the next nine-week session begins.[88] The district court found that the "manual has been and is vital to the commercial success of SE. It is a valuable property of SE and has always been treated as such by SE."[89]

In *Gold Messenger, Inc. v. McGuay*, the franchisor—which operated an advertising circular franchise system—sought and received a preliminary injunction against the franchisee and his life partner after they opened a competing concept within the same territory.[90] The franchise agreement contained a covenant not to compete for a period of three years and fifty miles from the territory of the franchised location.[91] Colorado, like other states, does not favor covenants not to compete. However, there are exceptions within the statute to this general rule. The statute cited by the Court of Appeals provides as follows:

> Any covenant not to compete which restricts the right of any person to receive compensation for performance of skilled or unskilled labor for any employer shall be void, but this subsection (2) shall

---

[82] *Id.* Defendant's owners went through the franchise training program and then worked as a moderator and registrar for the franchise system before leaving the system to open their own smoke cessation business. *Id.* at *5.

[83] *Id.*

[84] *Id.*

[85] *Id.*

[86] *Id.* In the early 1970's, smart phones were not being used, so "snapping" a picture with a phone during the program was not an option for attendees.

[87] *Id.*

[88] *Id.*

[89] *Id.*

[90] 937 P.2d 907, 908-09 (Colo. App. 1997).

[91] *Id.* at 909.

> not apply to . . . (b) Any contract for the protection of trade secrets. . . .[92]

The court determined that the franchise agreement "was a contract for the protection of trade secrets and, therefore, the covenant was valid under § 8–2–113(2)(b)."[93] The Court of Appeals, in determining that a trade secret did exist, held that "the purpose of the covenant must be the protection of trade secrets, and the covenant must be reasonably limited in scope to the protection of those trade secrets."[94] The Court of Appeals reviewed the preamble of the franchise agreement to determine that "the agreement was entered into with the express purpose of protecting trade secrets."[95] The 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; and
>
> 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 . . .
>
> WHEREAS, [Franchisee] has a full and adequate opportunity to be thoroughly advised of the terms and conditions of this Franchise Agreement by counsel of its own choosing; and
>
> WHEREAS, the parties wish to enter in the following terms and conditions of this Franchise Agreement.[96]

The Court of Appeals continued its analysis by taking both the language from the franchise agreement and the language from the non-compete provision and determining that the franchisee was precluded "from using the confidential information contained in the manual to compete unfairly against franchisor or other franchisees. Thus, by both its purpose and its scope, the

---

[92] *Id.* at 909 (quoting COLO. REV. STAT. § 8-2-113(2) (1986)).

[93] *Id.* at 910 (citing *Klipfel v. Neill*, 30 Colo. App. 428, 494 P.2d 115 (1972) (if trial court findings support its result under a different theory, appellate court may affirm judgment even though it rejects trial court reasoning)).

[94] *Id.* at 910 (citing *Mgmt. Recruiters of Boulder, Inc. v. Miller*, 762 P.2d 763 (Colo. App. 1988)).

[95] *Id.* at 910.

[96] *Id.*

covenant is, in essence, for the protection of trade secrets."[97] The Court of Appeals found that the franchisor took "'substantial steps to protect the confidential nature of the confidential Operations and Procedures manual, as well as to [protect] other information provided to its franchisees.'"[98]

In *Quizno's Corporation v. Kampendahl*, Quizno's sought a preliminary injunction against its former franchisee who—post termination—opened a similar sandwich restaurant in the exact same location as his franchised location.[99] Colorado law was the governing law under the franchise agreement. As discussed in *Gold Messenger*, Colorado's general prohibition of non-compete agreements contains an exception for the protection of trade secrets.[100] In the *Quizno's* case, the franchisee "acknowledged in the [Franchise] Agreement that anything revealed to him by Quizno's including the Operations Manual as well as Quizno's system in its entirety-constituted trade secrets."[101] The district court found sufficient likelihood of success on the merits for the issuance of a preliminary injunction.[102]

7. Prospective Franchisee Information

The identity of prospective franchisees and information about them were also considered protectable trade secrets in *Re/Max of America, Inc. v. Viehweg*.[103] The defendant former employee was hired as a sales broker for the Re/Max franchise system.[104] As a condition of his hiring, the defendant attended a one-week training course to learn about the system and represent the brand to potential and current franchisees.[105] One Saturday morning, the defendant went to the office and searched through various "desks, closets, and credenzas. . ." including the desk of his boss, and he "removed and read various documents and then took numerous

---

[97] *Id.* at 911 (citing *Mgmt. Recruiters of Boulder, Inc. v. Miller*, 762 P.2d 763).

[98] *Id.* The trial court also "noted" that the operations manual was copyrighted and the franchise agreement "expressly note[d] that the information, knowledge, and "know-how" contained in the manual are deemed confidential." *Id.*

[99] No. 01 C 6433, 2002 WL 1012997 (N.D. Ill. May 20, 2002).

[100] *Id.* at *6. The franchisor also argued that the non-competition provision should be enforceable under another exception as well, relating to the purchase and sale of a business. *Id.* at * 4.

[101] *Id.* at *6.

[102] *Id.* The district court determined that the non-competition provision "has the legitimate purpose of protecting Quizno's trade secret[s] in the Quizno's system and in the production of Quizno's sandwiches." *Id.*

[103] 619 F. Supp. 621 (E.D. Mo. 1985).

[104] *Id.* at 623.

[105] *Id.*

documents, papers, and records home with him."[106] The defendant was terminated after refusing to return the items.[107]

The defendant admitted "that he sought to launch a consulting business that would benefit Re/Max's competitors based at least in part on knowledge extracted from these materials."[108] The defendant contacted a number of the franchisor's competitors and offered to "sell . . . information which would help [them] to keep Re/Max or its franchisees from hiring away . . . real estate agents."[109] The defendant also sent mailings out to competitors in an effort to "solicit their hiring of him as a consultant who would show them how to keep Re/Max or its franchisees from hiring away their real estate agents."[110] The court found that "[i]n the course of his contacts and mailings with plaintiff's competitors and franchisees, defendant disclosed and relied upon the material Re/Max had given him as well as materials he took from the St. Louis office."[111] The court ruled that:

> Materials containing two years of referral rosters of franchised Re/Max offices and regional director/subfranchisor rosters including private home telephone numbers were developed over a period of many years, exclusively for the use of Re/Max personnel. Similarly, confidential lists of names of potential franchisees and confidential reports showing the sales produced by top sales associates and their commissions were compiled by plaintiff over a period and reflect a substantial investment of time and money by plaintiff, and Re/Max would suffer great competitive injury if these lists were to fall into the hands of competing franchisors who could then take advantage of Re/Max leads in their own franchising effort. [112]

The franchisor prevailed in its request for a temporary restraining order, which prohibited "defendant from disclosing any Re/Max trade secrets or proprietary information, and from communicating with anyone in any way about Re/Max. . . ."[113]

---

[106] *Id.* at 624. The defendant took these steps because he "became disenchanted with plaintiff's operations and voiced his concerns . . . " *Id.* at 623.

[107] *Id.*

[108] *Id.*

[109] *Id.*

[110] *Id.*

[111] *Id.* at 625.

[112] *Id.* at 626. The court ruled that not all of the materials that defendant received during the training session were trade secrets, but the court did find that some of the documents that defendant possessed were in fact trade secrets. *Id.* at 625-26.

[113] *Id.* at 625.

8. Product Line Extensions and Launch Dates

Franchise brands are constantly rolling out changes by extending the brand to new concepts, adding new menu items, offering new products, or expanding the services to be provided to the consumer. While not a franchise case, the holding in *Merck & Co., Inc. v. Lyon* relates to franchising because the court found information regarding a line extension for a product and prospective launch dates to be protectable trade secrets.[114]

Merck sought a preliminary injunction against its former employee and Glaxo Wellcome, Inc. (the company that the former employee started working for after leaving Merck).[115] The former employee had access to information that Merck claimed to be trade secrets surrounding Pepcid® AC, which at the time was a new drug being developed and launched by Merck.[116] Specifically, Merck claimed that the former employee "had access to trade secret information regarding projected launch dates and the development status of Pepcid® AC line extensions, or new dosage forms."[117] The district court found that the information about "projected launch dates" was not "generally known or readily ascertainable"[118] and the information regarding the drug line extension was "competitively valuable"[119] The district court pointed out that launch dates are "not always met" but this does not mean that there is no "competitive value" of knowing that information.[120] "Knowledge of projected launch dates, whether met or not, would allow Glaxo to determine plaintiffs' priorities and to competitively align their own priorities."[121]

In another matter that relates to an extension of a product line, among other alleged trade secrets, the court in *Static Control Components, Inc. v. Darkprint Imaging, Inc.* determined that the plaintiff could survive a motion to dismiss challenging the application of trade secrets to

---

[114] 941 F. Supp. at 1454.

[115] *Id.* at 1445. The employee was dismissed from the case for lack of personal jurisdiction. *Id.* at 1447.

[116] *Id.* at 1450.

[117] *Id.*

[118] *Id.*

[119] *Id.* The competitive advantage was due to the fact that Glaxo would be able to "prioritize and concentrate its efforts on certain Zantac® 75 [the new drug being developed by Glaxo] line extensions, enabling Glaxo to be first to market with competitive dosage forms." *Id.* In addition, the former employee had specific knowledge about "the status of various line extensions, including among other things problems encountered in developing new dosage forms, schedules for launching the different dosage forms, technologies being considered and their effect on launch dates, market research and positioning of the new dosage forms, and packaging." *Id.* Furthermore, the former employee also attended a number of meetings and received various minutes from meetings where discussions and decisions about the issues referenced in the preceding sentence were discussed. *Id.*

[120] *Id.* at 1451.

[121] *Id.* Furthermore, Merck claimed that the former employee also possessed knowledge about the launch of the Pepcid® AC product within Canada, and not only was that information a trade secret, but the district court agreed that "[t]his information is not generally known or readily ascertainable." *Id.* at 1453. The former employee "reviewed, revised and edited drafts of the Pepcid® AC marketing launch plan, which contained information such as planned expenditures in various areas." *Id.* The information relating to the launch dates "has competitive value for Glaxo because the knowledge of what plaintiffs' marketing strategy and plans are would allow Glaxo to determine how to market against plaintiffs." *Id.* at 1453.

plaintiff's "specialized knowledge" relating to developments within the toner business.[122] The plaintiff was in the business of distributing replacement toner cartridges and other parts for laser printers.[123] The defendant hired away five of the plaintiff's employees whom the plaintiff alleged had "specialized knowledge."[124] The district court found that there was commercial value in the "specialized knowledge" and that the plaintiff had taken steps to maintain the secrecy of the "specialized knowledge".[125]

Knowledge about launch dates for line extensions is a protectable trade secret. Although the above cases relate to a launch of a particular drug product and "specialized knowledge" regarding toner cartridges, their rationale is applicable to franchising. In franchising, an analogous situation would be where a franchise brand learned of a competitor's plans to launch a new meal, food, loyalty program, type of service, or product. Assuming that the information has value, is not generally known to the public, and has been kept secret, it will be afforded trade secret protection.

9. Supply Agreement

In *Merck & Co.,* the protectable trade secrets were not limited to launch dates and product extensions. The court also found that a company's supply agreement contained information that was a protectable trade secret.[126] Merck claimed that the former employee had such trade secret information regarding the active ingredient in Pepcid® AC.[127] The district court agreed with Merck and found that the former employee "had access to competitively valuable information regarding the nature of plaintiffs' famotidine supply agreement and its impact on plaintiffs' cost of goods, and that this information is not generally known or readily ascertainable."[128] The information about

---

[122] 135 F. Supp. 2d 722, 725 (M.D.N.C. 2001).

[123] *Id.* at 724.

[124] *Id.* at 727. The "specialized knowledge" was:

> a. development of toner especially for the remanufacturing process, which requires identifying and working with different manufacturers of toner to create a particular toner which works well with the components used by remanufacturers;
>
> b. customer support and technical assistance to remanufacturers working with a wide variety of laser printer cartridges, to address problems faced by remanufacturers;
>
> c. maintenance of a dedicated sales force with knowledge of specialized customer preferences and requirements in order to build customers' trust in existing products and new products extensions.

[125] *Id.*

[126] *Merck & Co., Inc.*, 941 F. Supp. at 1454.

[127] *Id.* at 1453.

[128] *Id.*

this ingredient would allow Glaxo (the competing company) "to determine plaintiffs' profit margin."[129]

In addition to the information within a supply agreement being a protectable trade secret, so too is the knowledge of the suppliers themselves, as detailed in *Proimos v. Fair Automotive Repair, Inc.*[130] The plaintiffs were franchisees of the Fair Automotive Repair franchise system. During the term of the franchise, the plaintiffs "repudiated their contracts with Fair, changed the names of their shops, and continued to sell mufflers at the same locations. . . ."[131] The franchisor filed, and lost, a motion for a preliminary injunction to prevent the franchisees from being in the muffler business.[132] The district court provided five reasons for denying the motion, the last one being "that the franchisees were using none of Fair's trade secrets."[133]

On appeal, the Seventh Circuit held that "[t]he court's conclusion that the franchisees are not using any of Fair's trade secrets also is questionable."[134] The franchisor "provided a great deal of information, from names of suppliers to the appropriate methods of replacing mufflers."[135] The franchisees, like most franchisees, agreed by contract to keep the information confidential and not to use it for competitive purposes, and the court added that "[i]nformation is the most valuable asset of many a business."[136] The district court observed "that much of the information could be observed or learned in some other way." The Seventh Circuit, however, held that this possibility "does not foreclose the possibility that the information is still a trade secret."[137] The appellate court provided the following example of how supplier information could be a trade secret: "suppliers of parts may be discovered by looking in a book, as the court emphasized, but the reliability of these suppliers and the terms on which they may be induced to deal may be valuable secrets."[138] Despite this possible example of trade secret protection, the court upheld the district court's denial of the preliminary injunction.[139]

---

[129] *Id.* The district court did determine that the amount of time this information would be a trade secret was limited since the supply agreement is subject to change.

[130] 808 F.2d 1273, 1275-76 (7th Cir. 1987).

[131] *Id.* at 1274.

[132] *Id.*

[133] *Id.* at 1275.

[134] *Id.*

[135] *Id.* at 1275-76.

[136] *Id.* at 1276.

[137] *Id.*

[138] *Id.* (citing *Greenberg v. FDA*, 803 F.2d 1213 (D.C. Cir. 1986)), in which a divided court debated whether information about who sells to whom is a trade secret. What divided the panel is whether this information has such obvious commercial value that it may be deemed a trade secret on summary judgment (as Judge Bork urged in dissent) or instead whether a trial was necessary to determine the degree of secrecy (as the majority concluded).).

[139] *Id.* at 1277. "Although the district court's findings do not make an airtight case for the denial of an injunction, Fair's arguments do not overcome the court's conclusions that Fair will not suffer irreparable injury from delay and that the

The disclosure of such trade secrets could cause the brand to lose its competitive edge, or market share, or valuable timing in trying to be first to market with a particular product, service, or offering. As discussed below, the steps taken to protect trade secrets and the mitigation plan in effect in the event of a disclosure are key to trying to protect the brand.

D. Non-Trade Secret Confidential Information and Third Party Data

Franchise systems maintain many types of confidential information that does not meet the definition of a "trade secret." This type of information can include third party data (such customer credit card data, personal identifiable information of employees, and protected health information). It can also include the confidential information of business partners, vendors, and suppliers and the franchise system's own franchisees. Regardless of whether certain proprietary data of vendors, suppliers, and franchisees qualify as trade secrets, the franchisor may be contractually obligated to maintain confidentiality. The same security breach by a departing employee or franchisee, a competitor, or a hacker may expose both the franchisor's own trade secrets and third party data. The legal remedies available for a data breach (other than breach of contract) may be the same regardless of whether it involves misappropriation of the franchisor's trade secrets or any unauthorized access to third party data, especially if stored electronically. These remedies are generally available regardless of whether the information accessed is a trade secret—or at least was before the breach. This is of critical importance because the breach itself (or subsequent dissemination and posting on the Internet) may cause the loss of trade secret status. Alternatively, if there is any chance of maintaining trade secret status, prompt pursuit of such remedies may be the only option.

III. COMMON SOURCES OF BREACH

When a cybersecurity breach involving third party data occurs, the typical bad actor is a hacker or thief unknown to the franchise system. Data breaches in franchise systems' computer networks can be a major source of exposure to claims brought by government enforcers[140] and private plaintiffs' attorneys, especially those specializing in class action litigation. Prompt pursuit of the wrongdoers—especially as a preemptive strike—may be an effective way of limiting such exposure, as discussed *infra* with respect to litigation options.

When a security breach occurs, the culprit is often a person or entity known to the franchisor. There are generally five sources of such breaches: (1) rogue or former franchisees; (2) former employees; (3) competing franchisors; (4) suppliers and vendors; and (5) third party bad actors. In most industries, former employees are by far the most common source of trade secret breaches. In franchising, former franchisees likely account for the lion's share of trade secret misappropriation claims. Examples of franchise cases involving the first three types of breaches follow.

---

grant of a preliminary injunction would greatly injure the franchisees by reducing to zero the value of their new trade names and business good will."

[140] *FTC v. Wyndham Worldwide Corp., et al.*, Case No. 2:13-CV-01887-ES-JAD (D.N.J. 2015).

A. Rogue or Former Franchisees

Often, claims for misappropriation of trade secrets and/or computer crimes are asserted by the franchisor in conjunction with claims against terminated franchisees. Trade secret and computer crimes claims are frequently joined with causes of action seeking to enforce de-identification requirements, non-competition covenants, and the like. For example, in *Jackson Hewitt, Inc. v. Barnes*, the franchisor sought and obtained a preliminary injunction requiring the terminated franchisee to remove Jackson Hewitt signage from Barnes' offices, transfer all Jackson Hewitt telephone numbers owned by Barnes to Jackson Hewitt, notify the telephone company that the franchisee no longer had the right to use such numbers, comply with the two year covenant not to compete, and return to Jackson Hewitt all client files.[141] That same month, the same franchisor obtained similar preliminary injunctive relief from the same court.[142] That franchisor obviously had a forum selection clause in its franchise agreement—a recommended "best practice."

Similarly, in *DLC DermaCare LLC v. Castillo*, the court found that the franchisor had adequately pled its claim for misappropriation of trade secrets.[143] The court so held because the franchisor had alleged the proprietary and confidential nature of the information (including manuals and marketing materials), that these materials had independent economic value by not being generally known by other parties, and that the franchisee continued to use the information after termination of the franchise agreements. Among the contractual provisions which the court based its holding was an acknowledgment by the franchisee that these materials were proprietary to the franchisor and constituted trade secrets.

These decisions underscore just how much the outcome of trade secret cases turns on the facts—including the importance of the alleged trade secret to the franchise concept, the measures taken by the franchisor to protect its secrecy, and the conduct of the franchisee alleged to constitute "misappropriation." Such factual differences account for the seemingly disparate outcomes in recent trade secrets cases involving former franchisees in which courts have:

- found insufficient evidence that a former franchisee was using the franchisor's trade secrets because the franchisor's recipes were publicly available;[144]

- denied preliminary injunctive relief against a former franchisee because "plaintiffs provide no specific details as to what trade secrets or confidential information were misappropriated, nor do they cite any evidence suggesting that such misappropriation is likely to have occurred;"[145]

---

[141] No. 10-cv-05108 DMC JAD, 2011 WL 181431 (D.N.J. Jan. 18, 2011).

[142] *See Jackson Hewitt, Inc. v. DJSG Utah Tax Serv., LLC*, No. 2:10-cv-05108 DMC JAD, 2011 WL 90311 (D.N.J. Jan. 10, 2011) and *Jackson Hewitt, Inc. v. H.E.A.T., LLC*, No. 10-cv-5108 DMC JAD, 2011 WL 63598 (D.N.J. Jan. 5, 2011).

[143] No. CV-10-333-PHX-DGC, 2010 WL 5148073 (D. Ariz. Dec. 14, 2010), *dismissed pending arbitration*, No. CV-10-333-PHX-DGC, 2011 WL 285825 (D. Ariz. Jan. 27, 2011).

[144] *D.P. Dough Franchising, LLC v. Southworth*, No. 2:15-cv-2635, 2017 U.S. Dist. LEXIS 157951, **27-33 (S.D. Ohio Sept. 26, 2017).

[145] *Golden Krust Patties, Inc. v. Bullock*, 957 F. Supp. 2d 186, 196 (E.D.N.Y. 2013).

- granted a permanent injunction as part of a default judgment on the basis that the defendants had published portions of the franchisor's admittedly confidential manual after termination of the franchise agreement;[146] and

- dismissing the franchisor's misappropriation of trade secrets claim against a former franchisee because the franchisor alleged no facts establishing that their alleged trade secrets have "independent economic value, actual or potential, from not being generally known" and "not being readily ascertainable by proper means,"[147] notwithstanding a prior decision by the same court finding that the franchisor's alleged trade secrets (in that case, a client list) qualified for trade secret protection.[148]

Typically, misappropriation of trade secret claims against former franchisees are asserted shortly after termination of the franchise. Sometimes, however, the facts giving rise to claims for misappropriation of trade secrets and computer crimes do not arise until years after termination. For example, the defendant in *NACCO Materials Handling Group, Inc. v. Lilly Co.*,[149] was a former dealer that had been terminated several years earlier and was now servicing a multi-state area on behalf of several competitors of plaintiff.[150] For several years after the termination, the defendant obtained unauthorized access to the plaintiff's "dealers only" secure Web site. The site contained proprietary information about pricing, diagnostic software, and other competitively sensitive materials. During a relatively early stage of the litigation, the court ordered the defendant to pay the plaintiff's attorneys' fees plus the cost of having a computer forensic expert image and analyze computers at the dealer's locations in Tennessee, Arkansas, Alabama, and Mississippi from which unauthorized access had been gained.

B. Former Employees

Sometimes, claims of misappropriation by a competitor arise when a franchisor's departing employees go to work for a competitor. For example, the plaintiff in *Starwood Hotels & Resorts Worldwide, Inc. v. Hilton Hotels Corp.*,[151] alleged that two former Starwood executives were using Starwood confidential information to develop a competing hotel brand known as "Denizen" on behalf of Hilton. The case ultimately settled on terms that included entry of a permanent injunction appointing an independent monitor to ensure that Hilton did not use any Starwood information. The injunction also prohibited Hilton from either buying or franchising any Starwood Lifestyle Brand hotel that Starwood operated, from hiring any Starwood employee for its Hilton Luxury & Lifestyle Brands Group (which includes Waldorf Astoria, Conrad Hotels &

---

[146] *Grout Doctor Global Franchise Corp. v. Groutman, Inc.*, No. 7:14-cv-105-BO, 2015 U.S. Dist. LEXIS 63960, **10-11 (E.D.N.C. May 15, 2015).

[147] *JTH Tax, Inc. v. Williams*, No. 2:18cv26, 2018 U.S. Dist. LEXIS 83011 *11 (E.D. Va. May 4, 2018).

[148] *JTH Tax, Inc. v. Harlan C. Hanson Enders*, No. 2:12cv625, 2013 U.S. Dist. LEXIS 192553 *7 (E.D. Va. March 25, 2013).

[149] 278 F.R.D. 395, 2011 (W.D. Tenn. 2011).

[150] Mr. Lockerby represented the plaintiff, NACCO Materials Handling Group, Inc.

[151] Case No. 8:09-cv-03862-JSG (S.D.N.Y.). The case was high profile but did not result in any reported decisions before it settled.

Resorts, and Denizen) for a period of two years, and from launching another brand similar to Denizen.

C. Competing Franchisors

In *Pop Bar, LLC v. Fellows*,[152] the plaintiff-franchisor alleged that the defendants explored the potential for becoming a franchisee for the purpose of obtaining the franchisor's valuable proprietary information to start a competing business. Because the defendants signed "a confidential disclosure agreement," Popbar shared with defendants the Popbar system, including Popbar's recipes and formulas, specially designed equipment, systems and methods of making customized Popbar products, and ideas for Popbar food trucks.[153] The court found that the franchisor's allegations of, *inter alia*, misappropriation of trade secrets and breach of the confidential disclosure agreement were sufficient to withstand a motion to dismiss.

One recent case in which a former franchisee went into competition with the franchisor is *Stockade Cos., LLC v. Kelly Restaurant Group, LLC.*[154] The defendant, a former franchisee of the plaintiff's "family-style buffets," rebranded the restaurant locations under a different trademark, as required by a prior preliminary injunction order. Besides seeking preliminary injunctive relief for infringement of its trade dress, the plaintiff-franchisor also sought preliminary injunctive relief against use of its confidential information in violation of the parties' franchise agreements and misappropriation of its trade secrets in violation of the Texas Uniform Trade Secrets Act. The court found that the franchisor's "buffet system" did not qualify as confidential information or a trade secret but rather was known to patrons and common in the industry. Another important factor in the court's decision was that the defendant no longer had access to the alleged confidential information of its former franchisor. It was also unhelpful to the plaintiff's case that the franchisor disposed of its allegedly secret documents (including recipes) in a public, unlocked dumpster.

IV. ALLOCATING RESPONSIBILITY IN THE EVENT OF A DATA BREACH[155]

A. Cyber Breaches at the Franchisee Level

When a breach incident occurs at the franchisee level (for example, by a cyber criminal hacking the franchisee's computers or by a former franchisee employee), most sophisticated franchise systems shift that risk of loss to the franchisee through protective provisions in the franchise agreement.[156] Indemnification provisions under the franchise agreement do not provide much comfort if there are no financial resources to pursue in the event of a breach incident. Therefore, most franchise systems now require their franchisees to maintain a cyber liability policy

---

[152] No. 12 Civ. 06647 (TPG), 2013 U.S. Dist. LEXIS 117739, 2013 WL 4446227 (S.D.N.Y. Aug. 19, 2013).

[153] *Id.* at *4.

[154] No. 1:17-cv-143-RP, 2017 U.S. Dist. LEXIS 170944, 2017 WL 4640445 (W.D. Tex. Oct. 16, 2017).

[155] The authors of this paper would like to thank the very knowledgeable agents at Marsh & McLennan Agency, Doug Imholte and Daniel Hanson, for their invaluable thoughts and insight on these issues.

[156] *See* Section VII.A.2 for suggested provisions for franchise agreement.

covering breaches from the theft, misappropriation, or disclosure of confidential or proprietary information. Cyber insurance policies are discussed in more detail in Section C below.

One unique issue in the franchise system context generating recent discussion in the industry is whether the franchisor should secure a master cyber insurance policy providing coverage for all franchisees. Some insurance carriers will underwrite master policies where the named insureds include both the franchise system and the franchisees. The master policy will have a large blanket aggregate limit that will be shared among all of the insureds. There are benefits to securing a master cyber policy. If there is a breach incident that involves multiple franchisees (for example, a cyber incident occurs in the Atlanta area affecting a dozen units), then the franchisor may want the ability to step in and control the investigation, litigate (if necessary), and attempt to mitigate the loss as quickly and efficiently as possible utilizing the service providers and counsel offered under the master policy issued by its insurance carrier. It may be easier to deal with one carrier and one policy rather than potentially twelve different carriers. Further, even if a franchisor determines that a single franchisee is at fault for a breach, the franchisee may not have the manpower or sophistication to properly address a data breach incident to the franchisor's satisfaction. This is particularly true where the breach involves sensitive trade secrets. It allows the franchisor to more effectively manage risk with one carrier under a blanket policy with a high limit. There are, however, limitations to a blanket policy that must be discussed with an insurance agent. For example, the "insured vs. insured" exclusion under a typical policy may limit a franchisor's ability to recover damages from a franchisee covered under the same blanket policy. Implementing these types of insurance plans should be done after careful consultation with a knowledgeable agent.

B. Cyber Breaches at the Vendor/Supplier Level

While employees and former franchisees are often the most common source of trade secret and proprietary information breaches, vendors are often a source of third party data breaches. When an investigation determines that a current or former vendor or supplier is responsible for a breach, then the franchisor should first review its agreement or contract with the vendor or supplier. In the best case, the agreement will clearly allocate liability for any vendor breaches to the vendor and require the vendor to indemnify and hold harmless the franchisor for any resulting losses. If there is not a blanket indemnification, then there may be indemnification available if the vendor failed to comply with laws and industry standards regarding the use, storage, and disclosure of sensitive and confidential information or was otherwise negligent in fulfilling its obligations under the agreement. Trade secret breach may constitute a breach of the vendor's service obligations under the agreement. As part of the review, the franchisor should also confirm that the vendor agreement contains no limits on liability, disclaimer of damages, or carve-outs to potential recoverable damages.[157]

The franchisor should also verify that the vendor submitted any claims to its insurance carrier. There are often three potential sources of insurance coverage when a data breach occurs at the vendor or supplier level:

- If the bad actor was a former employee or cyber hacker, then the vendor's standard cyber liability policy is likely triggered and should cover the claim so long as the vendor's policy covers not only the loss of the vendor's data but also the loss of a

[157] *See* Section VII.A.3 for suggested provisions to negotiate in vendor and supplier contracts.

third party's (in this case the franchisor's) confidential data and proprietary information held by the vendor.

- Many vendors (especially larger and more reputable vendors) carry professional liability (errors and omissions) policy that may insurance. E&O insurance provides coverage to a business for claims that the business acted negligently in providing its services to customers. Therefore, E&O policies sometimes cover claims resulting from losses cyber breaches resulting from a breach of confidential information of a in a loss of customer data while in the performance of its duties. The vendor should keep the franchisor updated and cooperate in the franchisor's investigation and potential litigation of the responsible parties.

- The third potential source of recovery is the franchisor's own cyber liability policy. Remember that a business cannot transfer the risk in the event of a data breach of third party personally identifiable information or personal health information to a vendor. The business outsourcing data collection, processing, transmission, or storage is still the "data owner" from a regulatory perspective. A franchise system can outsource the operations but cannot outsource the liabilities. Further, if the vendor becomes insolvent or goes bankrupt or just fails to abide by its contractual obligations, then the franchisor may be left on the hook.

Finally, indemnification and insurance alone cannot shift liability and should not lure a franchise system into a false sense of security. Franchise systems should always conduct due diligence on vendors. Examine the vendor's cybersecurity practices, use of encryption, and subcontractors. If it is a large vendor, then reserve audit privileges. Businesses can be liable for privacy violations and data breaches that arise from a vendor's unreasonable security practices[158]. Conduct a risk assessment by weighting the following: (1) type of data being shared; (2) how many records are involved (if protected health information ("PHI") or personally identifiable information ("PII"); (3) value of the contract or agreement; and (4) financial strength of the vendor to meet indemnity obligations.

Cyber policies and E&O policies do not cover intentional misconduct by an insured. If the vendor is the "bad actor" and that has misappropriated the franchisor's trade secrets or proprietary information of either the franchisor or a third party, then there is likely no vendor level insurance coverage to protect against the breach. It is also fairly unlikely that there is "offensive" insurance coverage to finance the legal action taken by the franchisor against the vendor. Some insurance carriers will offer abatement coverage. This is a specific type of "offensive" insurance coverage that will reimburse litigation costs and expenses incurred to pursue a misappropriating vendor. The insured (franchisor) and insurance carrier work together, and any proceeds received are shared between the franchisor and the insurer. This is not routinely offered by carriers, however. It is likely appropriate only in cases where (1) a franchise system is entering into a very large contract with a company like Microsoft where the risks of being out-financed and out-lawyered are great and (2) there is really top secret information at risk.

---

[158] Due diligence is particularly important with respect to approved or required vendors. Failure to properly evaluate a vendor's cybersecurity practices may expose a franchisor to claims by franchisees in the event of a system wide data breach.

C. Cyber Breaches at the Franchisor Level

As with any loss, the availability and adequacy of insurance coverage depends on the type of claim or loss the franchisor is seeking to have the carrier indemnify and/or defend. There are a number of insurance policies that may be triggered by a breach incident depending on whether the breach involves third party data or trade secret misappropriation or theft.

The franchisor's cyber insurance policy should provide coverage for third party claims (lawsuits filed against the franchisor) and first party losses (public relations costs, notifications, forensic investigations, payment card industry data security standard ("PCI-DSS") charges, and regulatory fines and penalties) arising from data breaches involving PHI, PII and other confidential information. Losses resulting from a data breach resulting in third party data (like customer lists) are likely covered under a standard cyber liability policy.

Losses resulting from the theft of trade secrets or proprietary information alone are unlikely to be insurable risks. Franchisors can purchase crime or employee theft policies to cover against losses resulting when an employee steals assets of his or her employer. Unfortunately, these policies rarely cover theft of a company intangible assets. If the franchisor can establish a direct connection between release of (intellectual property) and money lost, then crime insurance may cover the loss because it is not intangible.

What if the franchisor gets sued by its franchisees? When a breach occurs at the franchisor level, there is a legitimate risk that the system franchisees will feel the results financially. A franchise system can mitigate these risks by taking proper industry standard precautions to protect its trade secrets and third party data and by responding quickly and appropriately to an incident. Those precautions do not always eliminate the risk of franchisee lawsuits, however. If a franchise system is sued by its franchisees alleging that the franchisee suffered financial harm because the system failed to do something or did something it should not have done, then insurance coverage may exist under the franchisor's error and omissions policy. A franchisor's errors and omissions coverage provides defense and indemnification coverage for alleged mistakes, exclusions, or negligence in its provision professional services to its franchisees. If the definition of "professional services" is sufficiently broad, there may be coverage for such claims.

V. IMPLEMENTING A FRANCHISE SYSTEM'S BREACH RESPONSE PLAN

When a breach incident occurs despite a franchise system's best efforts to prevent it, a franchisor must be prepared to deal with it. Every franchise system should have a Data Incident Response Plan ("Response Plan") in place. Data breaches involving third party PHI, PII, and credit card data traditionally come to mind when thinking about Response Plans. However, a breach of trade secrets or confidential and proprietary information should also be part of any comprehensive franchise system Response Plan. The Response Plan should contain various alternatives based upon the type of data released or stolen (trade secrets; customer credit card information, PHI or PII; or employee data) and the type of breach (employee misconduct, franchisee level breach, accidental—like the loss of a laptop). The last thing a business wants to do is spend precious time spinning its wheels while it decides how to handle a breach event. Further, response speed is a factor that a franchise system can use to establish it has a

protectable interest in the trade secrets in the event of a trade secret misappropriation claim.[159] Below are the pre-litigation steps that every franchise system should take when it discovers that it may be the victim of a data breach.

A. Gather and Alert the Whole Response Team

If the franchise system has a Chief Privacy Officer or Trade Secrets Compliance Officer, then that executive should work with management to designate a committee or core group of professionals who will work to investigate and respond to the data breach. The committee should include in-house general counsel, outside counsel (in the event litigation is required), and a representative from the company's information technology ("IT") group who will work with legal, forensics, and management to determine the cause and scope of the breach and how to mitigate loss. Each employee in the response group should have detailed responsibilities. A franchise system may modify the members of a committee depending on the type of breach (trade secrets vs. third party data). This step should be completed within hours of discovering that a data breach occurred or may have occurred.

B. Identify the Compromised Information and Scope of Breach

The next step is to identify the compromised information and the scope of the breach. Identifying the type of compromised information will help the committee determine the steps that must be taken to contain the loss.

If the breach includes personally identifiable information or other third party data, then the team should take immediate steps to determine what type of data was compromised, the size of the data compromised or potentially compromised, when the incident occurred and whether the incident is continuing. Especially in the case of personally identifiable information, it is critical that this step is completed within the first 24 hours or as soon as reasonably possible so that the committee can move quickly to notifying affected individuals (as described below). Timely notification to affected individuals is crucial. Certain state or federal statutes may set time periods under which a business must notify a victim of a potential breach of his or her information. Regardless, however, of the regulatory considerations, each passing hour increases the risk that the data will be used by a bad actor improperly.

In the case of trade secrets or misappropriation the analysis is different. If a former franchisee places a copy of the franchise system's operations manual on the Internet, then this step may appear straightforward, but this is not always the case. Many franchise systems do not have a structure in place to identify, value, and protect all of the confidential information that may constitute "trade secrets." Failing to methodically and comprehensively identify all of the trade secrets or third party data that were compromised may affect the legal team's ability to take all appropriate action.

If the source of the breach is a former employee, then an in-depth forensic analysis of the perpetrator's email, computer and electronic devices, office access records, telephone calls, and travel and expenses records is appropriate. In many cases, the franchisor's internal IT group may

---

[159] Kevin Cloutier, Shawn Fabian, Mikela Sutrina and Amy Harwath, *Employer Cybersecurity Measures For Trade Secret Protection,* Law360, May 11, 2017, available at https://www.law360.com/corporate/articles/922706?utm_source=shared-articles&utm_medium=email&utm_campaign=shared-articles.

not have such capabilities, so engaging an outside experienced forensic investigator is appropriate.

Further, if the security breach involves personally identifiable information or other third party data (as in the case of a theft of customer lists), then the franchisor must implement additional response steps. These steps will include all those contained in a traditional data breach response plan such as notifying and communicating with affected individuals. Understanding whether third party information was compromised by a trade secrets breach allows the franchisor to tailor its response steps.

C. Bring in the Reinforcements

Whether the breach involves third party data or trade secrets, there is likely an outside support team and other parties to notify and involve in the process. The franchise system should notify law enforcement.[160] It should also strictly follow the process outlined in its insurance policies for notifying insurance carriers of the breach to ensure coverage is available under any applicable insurance policies. Depending on the type of breach and insurance coverage available, there may be multiple policies triggered in the event of an incident (cyber, franchisor errors and omissions, crime). Timely notice of an incident giving rise to coverage under a policy is a condition to coverage under any policy so involve legal and talk to the franchise system's insurance agent to ensure notice is timely and properly given. If there are other third parties that require notice pursuant to an agreement or contract, then notify those parties. These parties may include certain business partners, credit card brands and banks. This is also the time to engage and notify any forensic investigators. Keep in mind that many cyber insurance policies have designated and approved vendors so talk to your agent or carrier before engaging your own investigator. This step should be completed at least within the first 48-72 hours of a data breach, if not sooner.

D. Identify the Bad Actor or Responsible Party

The next step is identifying the bad actor or responsible party. In the case of a trade secrets breach, in most cases the source will be a former employee or former franchisee. However, if the breach was caused by a cyber criminal, then take steps to identify the wrongdoer. If the source of the breach is at the franchisee level, then determine how the franchisor and franchisees should work together to respond to the breach. Especially in the case of breaches involving third party data, this is not the time to assign blame to a particular franchisee or for a franchisee or franchisees to assign blame to the franchisor. Franchise systems are in a unique position with respect to third party data breaches (especially credit card information) because these breaches often occur at the point-of-sale system level. If the system requires the use of an approved POS System vendor, then blame can quickly shift to the franchisor, even if the franchisee was negligent in its practices and procedures. A franchise system should focus on mitigating loss and complying with statutory, contractual and other legal requirements. If the breach occurs at the vendor level, then the franchisor should analyze its rights under its agreement with the vendor and, where applicable: confirm the vendor notified its insurance

---

[160] There are many conferences and programs throughout the USA at any given time focusing on security and cyber security breaches. Often there will be an opportunity to hear from an FBI agent or specialist working in a cyber security crime division. We strongly suggest that a franchise system's in house counsel or privacy officer take the opportunity to hear a law enforcement officer speak and educate themselves on how law enforcement can work with a franchise system in the event of a breach. It may assuage fears that many businesses have regarding the involvement of law enforcement when these incidents occur.

carriers; exercise any rights to indemnification; determine which party will take responsibility for complying with notice laws, notifying victims, providing credit monitoring and leading the defense of any eventual lawsuits.

E. Preserve and Chronicle Every Detail of the Breach

The Response Plan should mandate a detailed chronology of the breach, misappropriation, or theft and all actions taken to respond. This information can assist in both criminal and civil proceedings against those responsible. In addition, the timeline and details regarding the steps taken by the franchisor will be critical in the event of later litigation to establish that the franchisor took reasonable steps to protect its trade secrets. If the cyber breach includes or involves third party data, then this timeline will be critical in the event that there are memories can be refreshed in the event of later litigation or governmental investigations. If the investigation reveals a vulnerability that can be corrected, the franchisor should do so. This is the right thing to do on every level, and evidence of subsequent remedial measures is typically not admissible to prove negligence.

When a data breach occurs, also always keep in mind attorney-client privilege issues and work to maintain the confidentiality of communications where legal advice is given so privilege is not waived. This is particularly relevant with a franchise system's internal IT or IS team who may not be sensitive to privilege issues and may not think twice about emailing out a message without regard to which individuals are copied.

F. Notify Affected Individuals (the Victims)

As soon as possible after completing the above steps, the franchise system should focus on external communications. The franchise system should notify affected individuals in compliance with all breach notice statutes. There is not one single federal law that governs the collection, storage, use and disclosure of personally identifiable information and the remediation obligations of a business in the event of a data breach but almost all states have enacted legislation requiring businesses to notify individuals of security breaches of information involving PII. Again, remember that the business that owns the customer, owns the response. Even if a franchise system can shift the responsibility to a vendor or other third party, the ultimate liability for compliance will rest with the business that owns the customer.

Coordinate these statutory notifications with other public relations efforts, including social media posts, press releases, and other media outreach.

G. Exercise Pre-Litigation Remedies

When appropriate, the franchisor may take the preliminary step of sending a cease and desist letter to the former employee or franchisee reminding the wrongdoers of their contractual obligations to the franchisor, demanding them to cease from engaging in the conduct, and requiring them to return any trade secrets or other confidential or proprietary information immediately and take whatever steps can be taken to remedy the breach and mitigate damage. In the case of a former employee who is misappropriating trade secrets in connection with his or her new employment, the franchisor may send a cease and desist letter to the new employer. Similarly, if a former franchisee is misappropriating trade secrets in connection with its operation of a new franchise in a competitive system, then a cease and desist letter to the competing franchise system may be appropriate. Such demand letters may also be appropriate in case of a third party breach.

The franchisor may also consider contacting law enforcement when criminal conduct is suspected. The threat of a criminal investigation may be enough to get the former employee or franchisee to cooperate and may defer other attempts to misappropriate the franchisor's trade secrets. The franchise system has to weigh these benefits against the potential of disclosure during the prosecution of a case.

H. Take Legal Action.

Determine whether legal action is appropriate. The next section of this paper will discuss the potential legal options available to a franchise system when a breach or theft of trade secrets or confidential information occurs.

VI. LITIGATION OPTIONS

A. Overview of Available Remedies

Of the various potential causes of action available, most offer similar remedies. The principal differences arise in the elements of the cause of action and their applicability to the facts. The remedies available under the various common law doctrines and statutes discussed in this paper are as follows:

POTENTIAL CAUSE OF ACTION	AVAILABLE REMEDIES			
	Preliminary injunction	**Compensatory damages**	**Costs and attys' fees**	**Other remedies**
Uniform Trade Secrets Act ("UTSA")	✓	✓	✓	
Federal Defend Trade Secrets Act ("DTSA")	✓	✓	✓	*Ex parte* seizure orders
Federal Computer Fraud and Abuse Act ("CFAA")	✓	✓	✓	
State "Computer Crimes" Statutes	✓	✓	✓	Sealing the record
Federal Electronic Communications Privacy Act ("ECPA")	✓	✓	✓	

Even in cases involving breach of third party data, trade secret remedies may be appropriate if the breach involved trade secrets of a third party. In any case involving a cybersecurity breach, claims under CFAA, state "computer crimes" statutes, and ECPA are critical. This is true even in trade secret cases, since the breach may have caused loss of trade secret protection.

B. Federal Defense of Trade Secrets Act

Effective May 11, 2016, a pre-existing criminal statute protecting trade secrets—the Economic Espionage Act of 1996, 18 U.S.C. §§ 1831-1839—was amended to provide private litigants with a civil cause of action. These amendments were contained in the federal Defend Trade Secrets Act of 2016 (the "DTSA"). The DTSA tracks the UTSA in many respects, but there are also several key distinctions.

The DTSA adopts with minor changes the definition of "trade secret" included in the Economic Espionage Act, 18 U.S.C. §§ 1831-39, the criminal statute that the DTSA amended to add a civil remedy. Under the DTSA, a "trade secret" is defined as:

> [A]ll forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—
>
> > (A) the owner thereof has taken reasonable measures to keep such information secret; and
> >
> > (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.[161]

The DTSA definition of "trade secret" closely tracks the UTSA definition. However, some federal courts have noted that the definition used in the DTSA is broader in scope because it expressly includes "all forms and types" of information, lists several types of information that are not present in the UTSA definition, and expressly covers tangible and intangible information.[162] This definition thus may cover information that falls outside the scope of the UTSA as it has been applied in some states, such as discount or pricing information listed in a format that does not qualify as a "formula" or "compilation."[163]

The DTSA provides civil and criminal immunity to employees for confidential disclosure of trade secrets to the government or to an attorney when such disclosure qualifies as

---

[161] 18 U.S.C. § 1839(3) (as amended by the DTSA).

[162] *U.S. v. Martin*, 228 F.3d 1, 11 (1st Cir. 2000); *U.S. v. Hsu*, 155 F.3d 189, 196 (3d Cir. 1998).

[163] *Neal v. Griepentrog*, 108 Nev. 660, 837 P.2d 432, 435 (1992) (information about discounts and pricing information between hospital and preferred provider organizations contained in letters sent to State Department of Human Resources was not a trade secret under the UTSA because it was not a "formula, pattern, compilation, program device, method, technique or process"); *N. Highland Inc. v. Jefferson Mach. & Tool Inc.*, 2016 WI App 41, 369 Wis. 2d 223, 880 N.W.2d 182, *review granted*, 2016 WI 98, 372 Wis. 2d 274, 891 N.W.2d 407, and *aff'd,* 2017 WI 75, 377 Wis. 2d 496, 898 N.W.2d 741, *reconsideration denied*, 2017 WI 94, 378 Wis. 2d 225, 904 N.W.2d 373 (confidential bid amount was not a trade secret because it was not among the types of information listed in the UTSA).

"whistleblowing."[164] The DTSA requires that any employee or contractor agreement concerning the use of trade secret or other confidential information must contain notice of this whistleblower immunity. Failure to provide such notice may leave the employer unable to pursue exemplary damages or attorneys' fees in an action against an employee or contractor under the DTSA.[165]

The UTSA does not fully define "improper means." Instead, it provides some nonexclusive examples. These include "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means." The DTSA's definition of "improper means" is substantively similar.[166]

Although the federal DTSA does not reject the doctrine of inevitable disclosure altogether, it is consistent with the trend of judicial reluctance to apply the inevitable disclosure doctrine in the absence of other evidence. Injunctive relief under the DTSA cannot "prevent a person from entering into an employment relationship" and cannot "conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business."[167] Injunctive relief cannot restrict an individual's employment based "merely on the information the person knows" but instead must be "based on evidence of threatened misappropriation."[168]

C. Preliminary Injunctive Relief (Including *Ex Parte* Seizure Orders)

Preliminary injunctive relief is typically the most effective remedy for trade secret misappropriation and third party data breach whatever the cause of action. Under the Restatement, "a defendant's continuing or threatened use or disclosure of a trade secret normally justifies an award of injunctive relief."[169] Indeed, where a trade secret has not been disclosed or used, an injunction may be the ***only*** appropriate remedy.[170] The Uniform Trade Secrets Act and Defend Trade Secrets Act have similar provisions. Both statutes expressly authorize preliminary injunctive relief.

An implicit prerequisite for injunctive relief, under the UTSA and generally, is that the trade secret owner must identify the alleged trade secrets with reasonable specificity or particularity.[171] This requirement arises out of a matter of fairness: a defendant accused of misappropriation cannot mount a defense without being advised regarding the identity of the alleged trade secret. Although a plaintiff may not be required to make this identification in the initial pleading, the party

---

[164] 18 U.S.C. § 1833(b)(1) (as amended by the DTSA).

[165] 18 U.S.C. § 1833(b)(3) (as amended by the DTSA).

[166] 18 U.S.C. § 1839(6) (as amended by the DTSA).

[167] 18 U.S.C. § 1836(b)(3)(A)(i)(I) (as amended by the DTSA).

[168] *Id.*

[169] Restatement (Third) of Unfair Competition § 44 (1995) at 500.

[170] *Id.*

[171] *See, e.g., Nilssen v. Motorola, Inc.*, 963 F. Supp. 664, 672 (N.D. Ill.1977) ("[A trade secret owner] must articulate protectable trade secrets with specificity or suffer dismissal of his claim." (citation omitted)).

claiming misappropriation of trade secrets will have to provide such identification in a confidential interrogatory answer or a separate confidential pleading.[172]

In addition to prohibitory injunctions, provision of complete relief may necessitate a mandatory 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. Restatement, comment (c) at 500. Section 2(c) of the UTSA authorizes the entry of court orders, in appropriate circumstances, that compel "affirmative acts to protect a trade secret."[173] For example, a court may order a defendant to return trade secrets or to recall and destroy products made from and containing the misappropriated trade secret. The DTSA similarly permits the issuance of mandatory injunctive relief.[174]

A primary purpose of preliminary injunctive relief is to preserve the status quo pending trial "for otherwise effective relief may become impossible...."[175] In this regard, the status quo to be preserved is the last, actual peaceable uncontested status that preceded the pending controversy.[176] Thus, the fact that the party against which 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.[177] However, the fact that trade secrets have already been disseminated may mean that preliminary injunctive relief is not available—at least not for misappropriation of trade secrets. Under this scenario, preliminary injunctive relief may still be available under alternative causes of action—especially federal and state computer crimes statutes.

Preliminary injunctive relief typically requires notice to the adverse party. 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:[178] "The court may issue a preliminary injunction only on 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.[179] In addition, federal laws protecting other forms of intellectual property provide for *ex parte* seizure orders under certain circumstances. For example, the federal trademark

---

[172] *Id.* at 673.

[173] UTSA § 2(c) (1985).

[174] 18 U.S.C. § 1836(b)(3)(A)(ii) (as amended by the DTSA).

[175] *Blackwelder Furniture Co. v. Seilig Mfg. Co.*, 550 F.2d 189, 194-95 (4th Cir. 1977). *Blackwelder* no longer governs the issuance of preliminary injunctions in the Fourth Circuit because of the Supreme Court's decision in *Winter v. Natural Res. Def. Council*, 555 U.S. 7 (2008). *See Real Truth About Obama, Inc., v. Fed. Election Comm'n*, 575 F.3d 342, 346 (4th Cir. 2009), *cert. granted, judgment vacated on other grounds*, 559 U.S. 1089 (2010), *reissued in relevant part*, 607 F.3d 355 (4th Cir. 2010). *Blackwelder* does remain good law, however, to the extent that it states the purpose of preliminary injunctive relief.

[176] *Hydroaire, Inc. v. Sager*, 98 Ill. App. 3d 758, 424 N.E. 2d 719 (1981).

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

[178] *See* Fed. R. Civ. P. 65(a)(1).

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

statute, the Lanham Act, contains special provisions for *ex parte* seizure orders with respect to counterfeit marks.[180] The Copyright Act authorizes temporary injunctive relief, impoundment of infringing articles, and—in the case of federal criminal prosecutions—seizure and forfeiture.[181]

Before enactment of the Defend Trade Secrets Act, there was no federal statute comparable to the Lanham Act and Copyright Act allowing a private right of action for misappropriation of trade secrets. With the enactment of the DTSA, a federal statute now authorizes preliminary injunctive relief—including *ex parte* seizure orders—for the misappropriation of trade secrets. Under the DTSA, an *ex parte* seizure order can be obtained where: (1) an injunction entered after the provision of notice that Federal Rule 65 ordinarily requires would be inadequate, as the subject of the order would "evade, avoid, or otherwise not comply with such an order;" (2) immediate and irreparable injury will occur in the absence of a seizure; (3) the harm of denying the seizure outweighs the harm to the legitimate interests of the person against whom seizure would be ordered, and substantially outweighs the harm of seizure to third parties; (4) the applicant is likely to succeed in showing that the information at issue is a trade secret, and the subject of the seizure order misappropriated or conspired to misappropriate the trade secret; (5) the subject of the order actually possesses the trade secret and any property to be seized; (6) the application describes the matter to be seized and its location; (7) the subject of the order, or someone in concert with the subject of the order, would destroy, hide, or otherwise make inaccessible to the court the information at issue if notice were given; and (8) "the applicant has not publicized the requested seizure."[182]

In addition, the combination of the Federal Rules of Civil Procedure and state law can be used to accomplish the same result. As previously discussed, Federal Rule 65(b) does specify circumstances under which *ex parte* temporary injunctive relief is warranted. In addition, Federal Rule 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.[183] These state law remedies also include those available under trade secret law. The UTSA specifically authorizes mandatory injunctions requiring the return of all tangible embodiments of the trade secrets, as does the Restatement.[184]

Depending upon the sensitivity of the trade secret, expedited trial may be a viable alternative to preliminary injunctive relief. If the parties consent to an expedited trial on the merits, the consent order can and should include a provision whereby the parties agree to preserve the status quo pending trial. The Federal Rules also contemplate motions for expedited discovery.[185]

---

[180] *See* 15 U.S.C. § 116(d).

[181] 17 U.S.C. §§ 502, 503, and 509.

[182] 18 U.S.C. § 1836(b)(2)(A)(ii) (as amended by the DTSA).

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

[184] UTSA § 2(c); Restatement (Third) of Unfair Competition, Chap. 4, § 44 comment (e) at 503 (1995).

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

In addition, the Federal Rules specifically allow the preliminary injunction hearing to be consolidated with the trial on the merits. Fed. R. Civ. P. 65(a)(2).

Preliminary injunctive relief typically requires a bond to protect the adverse party in case the injunction is later vacated.[186] Preliminary injunctive relief needs to be specifically tailored to the conduct at issue. Fed. R. Civ. P. 65(d) requires that a TRO or preliminary injunction "state the reason why it issued," "state its terms specifically," and "describe in reasonable detail -- and not by referring to the complaint or other document -- the act or acts restrained or required." In other words, general prohibitions against using or disclosing trade secrets are too vague and too broad. The moving party should submit a proposed preliminary injunction order, findings of fact, and conclusions of law.

The effect of the preliminary injunction is not necessarily limited to parties to the litigation. Once preliminary injunctive relief has been entered, the order is binding upon the . . . parties (including their "officers, agents, servants, employees, and attorneys") ***and*** upon those "persons who are in active concert or participation with anyone described in Rule 65(d)(2)(A) or (B)."[187] To expand the reach of the injunction beyond the enjoined parties, the party obtaining the injunction can and should serve copies upon "those persons who are active concert or participation" with them.

Franchisors seeking preliminary injunctive relief should not lose sight of the fact that this relief is discretionary. The federal courts enjoy considerable discretion whether to grant preliminary injunctive relief.[188] 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.

Both the UTSA and the DTSA authorize royalty order injunctions. The UTSA gives a court the flexibility to tailor equitable relief to meet the particular circumstances of the parties relative to each other. Specifically, "[i]n exceptional circumstances, an injunction may condition future use upon payment of a reasonable royalty for no longer than the period of time for which use could have been prohibited."[189] "Section 2(b) deals with the special situation in which future use by a misappropriator will damage a trade secret owner but an injunction against future use nevertheless is inappropriate due to exceptional circumstances."[190] In such "exceptional circumstances," the court may choose to grant a "royalty order injunction" that conditions the defendant's future use of the trade secret upon the payment of a reasonable royalty to the plaintiff

---

[186] *See* Fed. R. Civ. P. 65(c) ("The court may issue a preliminary injunction or a temporary restraining order only if the movant gives security in an amount that the court considers proper to pay the costs and damages sustained by any party found to have been wrongfully enjoined or restrained. The United States, its officers, and its agencies are not required to give security.").

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

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

[189] UTSA § 2(b) (1985).

[190] *Id.* cmt. at 8.

instead of a prohibitory injunction that bars future use by the defendant.[191] The DTSA contains a similar provision, permitting the court in "exceptional circumstances that render an injunction inequitable" to condition future use of another's trade secret on the payment of a reasonable royalty.[192]

One example of "exceptional circumstances" arises in the case of an innocent misappropriator who acquires certain information in good faith and without actual or constructive knowledge that that information constitutes a trade secret belonging to another.[193] If the misappropriator then makes use of the information such that the subsequent entry of a prohibitory injunction would be prejudicial, a royalty order injunction may be awarded instead. This remedy, however, is not intended to immunize all bona fide purchasers who have paid value in good faith for trade secret information wrongfully acquired by another person.

D. Federal and State Computer Crimes Laws

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 e-mail). 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 supplier need not prove the existence of trade secrets. As previously discussed, the fact that a "hacker" was successful makes it more difficult for the supplier to establish the reasonableness of it 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.

1. Computer Fraud and Abuse Act

The federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA"), prohibits intentional access to a computer without authorization or beyond the scope of any authority. The 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." Does the "interruption of service" requirement 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

---

[191] *Id.* at 9.

[192] 18 U.S.C. § 1836(b)(3)(A)(iii) (as amended by the DTSA).

[193] UTSA § 2(b) (1985) ("Exceptional circumstances include, but are not limited to, a material and prejudicial change of position prior to acquiring knowledge or reason to know of misappropriation that renders a prohibitive injunction inequitable.").

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."[194] 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).[195] 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.[196]

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 [the plaintiff]'s confidential, trade-secret information, which has damaged [the plaintiff]'s business interests."[197] 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."[198] In contrast, that same court has since found sufficient for purposes of Rule 12(b)(6) the allegations of a complaint that the 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."[199] The allegations of "damage" that the court found sufficient included the allegation that the defendant's actions had caused the plaintiff to "institute remedial measures and restore the computer system to the condition it was in prior to the alleged damage."[200] The court so held considering the "liberal pleading standard and the Court's standard of review for a motion to dismiss."[201]

---

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

[195] *Id.* at 645.

[196] *Barnstormers, Inc. v. Wing Walkers, LLC*, No. EP-10-CV-261-KC, 2011 U.S. Dist. LEXIS 47143, at *29–30 (W.D. Tex. May 3, 2011) (internal quotation and citation omitted); *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") (internal quotation omitted)); *SuccessFactors, Inc. v. Softscape, Inc.*, 544 F. Supp. 2d 975, 980 (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).

[197] *ReMedPar, Inc. v. AllParts Med., LLC*, 683 F. Supp. 2d 605, 614 (M.D. Tenn. 2010).

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

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

[200] *Id.* at *25.

[201] *Id.* at *23.

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.[202]

Regardless of whether it is directed at the company's own trade secrets, conduct that can violate CFAA includes:

- unauthorized access to Web sites[203];
- using extractor software to "harvest" e-mail addresses[204];
- diversion of customers, including the use of "bots" to gather customer lists and pricing information[205];
- defective software that causes damage to data, including undisclosed disabling code a/k/a "logic bombs"[206]; and
- intentional placement of cookies and other devices used to breach privacy.[207]

In recent years, CFAA has become a preferred method of seeking injunctive relief, damages, attorneys' fees, and other remedies from disloyal employees, competitors, and others—including distributors, dealers, and franchisees—who have made improper use of proprietary information stored on the company's computer system, or destroyed electronically stolen information altogether. For example, the Seventh Circuit held several years ago that an employee who erased crucial data on his company laptop before turning it in at the end of his employment violated CFAA.[208] The Seventh Circuit reasoned that the employee had violated CFAA's prohibitions against using a computer "without authorization" and in a manner that "exceeds authorized access."

Two leading federal appeals court decisions, however, have raised questions about the viability of CFAA as a remedy for such misconduct. In *WEC Carolina Energy Solutions LLC v.*

---

[202] *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*, No. 2:05-cv-00108-JTM-APR, at *12–13 (N.D. Ind. Mar. 31, 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).

[203] *See, e.g., EF Cultural Travel BV v. Explorica*, 274 F.3d 577, 578-79 (1st Cir. 2001).

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

[205] *See, e.g., YourNetDating, Inc. v. Mitchell* 88 F. Supp. 2d 870, 870-72 (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); *Sw. Airlines Co. v. Farechase Inc.*, 318 F. Supp. 2d 435 (N.D. Tex. 2004).

[206] *See, e.g., 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*, No. SA CV 96-71AHS(EEX), 1996 WL 1359212 at *7 (C.D. Cal. Aug. 19, 1996).

[207] *See, e.g., 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).

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

Miller,[209] 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. 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 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 involved a computer.

The Fourth Circuit's July 26, 2012 decision in *WEC Carolina* expressly adopted the rationale of an April 2012 *en banc* decision of the Ninth Circuit. Authored by former Chief Judge Kozinski, the Ninth Circuit's decision in *United States v. Nosal*,[210] reversed a three-judge panel's decision that was consistent with the Seventh Circuit's more expansive view of CFAA. CFAA, the Ninth Circuit held in Nosal, provides no remedy against a group of disloyal employees who retrieved confidential information via their company user accounts and transferred it to a competitor. 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."

Whatever the merits of the recent CFAA decisions by the Fourth and Ninth Circuits, they make one prospect seem likely: The Supreme Court may be called upon to resolve conflicting views of the scope of CFAA. Meanwhile, neither of these two decisions would affect the viability of a CFAA claim against a true "hacker."

Moreover, the Fourth Circuit itself has since distinguished the WEC *Carolina* decision. In *United States v. Steele*,[211] the Fourth Circuit held that the employer's failure to change an employee's password after he resigned did not mean that it intended for him to have access to the information after he resigned. The employee's ongoing access was therefore "in excess of authorization" within the meaning of 18 U.S.C. § 1030 (a)(2) for purposes of a criminal CFAA prosecution. Even in the Fourth Circuit, therefore, CFAA continues to provide a viable remedy vis-à-vis ***former*** employees (and presumably former franchisees).

2. State Computer Crime Laws

State computer crimes laws prohibit "use" of computers "without authority." If the particular state statute does not afford a private right of action, the claim can be combined with a cause of

---

[209] 687 F.3d 199, 202-03 (4th Cir. 2012).

[210] 676 F.3d 854, 863-64 (9th Cir. 2012).

[211] 595 Fed. App'x. 208 (4th Cir. 2014).

action for common law trespass. The remedies typically available include sealing the record, injunctive relief, and costs and attorneys' fees. For example, the Virginia Computer Crimes Act, Va. Code § 18.2-152.1 *et seq.*, 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 attempts to cause or causes a computer or computer network to perform or to stop performing computer operations;[212]

"Without authority" is defined as follows: "A person is 'without authority' when he knows or reasonably should know that he has no right, agreement, or permission or acts in a manner knowingly exceeding such right, agreement, or permission.[213]

The specific offenses prohibited by the Virginia Computer Crimes Act—all of which involve "use" of a computer "without authority"—are computer fraud, computer invasion of privacy, theft of computer services, and personal trespass by computer. "Computer fraud" is defined as follows:

> Any person who uses a computer or computer network without authority and:
>
> 1. Obtains property or services by false pretenses;
>
> 2. Embezzles or commits larceny; or
>
> 3. Converts the property of another; is guilty of the crime of computer fraud. If the value of the property or services obtained is $500 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 $500, the crime of computer fraud shall be punishable as a Class 1 misdemeanor.[214]

"Computer trespass" is defined as follows:

> A. It shall be unlawful for any person, with malicious intent, to:
>
> 1. Temporarily or permanently remove, halt, or otherwise disable any 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;

---

[212] VA. CODE § 18.2-152.2(4).

[213] *Id.*

[214] *Id.* § 18.2-152.3.

3. Alter, disable, 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. Use a computer or computer network to cause physical injury to the property of another;

6. Use a computer or computer network to 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;

7. [Repealed];

8. Install or cause to be installed on the computer of another, computer software for the purpose of (i) taking control of that computer so that it can cause damage to another computer or (ii) disabling or disrupting the ability of the computer to share or transmit instructions or data to other computers or to any related computer equipment or devices, including but not limited to printers, scanners, or fax machines.

9. Install or cause to be installed on the computer of another, computer software for the purpose of (i) taking control of that computer so that it can cause damage to another computer or (ii) disabling or disrupting the ability of the computer to share or transmit instructions or data to other computers or to any related computer equipment or devices, including but not limited to printers, scanners, or fax machines.

B. Any person who violates this section is guilty of computer trespass, which shall be a Class 1 misdemeanor. Any person who violates this section for the purposes of affecting a computer that is exclusively for the use of, or exclusively used by or for, (i) the Commonwealth or any local government within the Commonwealth or any department or agency thereof or (ii) a provider of telephone, including wireless or voice over Internet protocol, oil, electric, gas, sewer, wastewater, or water service to the public is guilty of a Class 6 felony. If there is damage to the property of another valued at $1,000 or more caused by such person's act in violation of this section, the offense shall be a Class 6 felony. If a person installs or causes to be installed computer software in violation of this section on more than five computers of another, the offense shall be a Class 6 felony. If a person violates subdivision A 8, the offense shall be a Class 6 felony.

C. Nothing in this section shall be construed to interfere with or prohibit terms or conditions in a contract or license related to

computers, computer data, computer networks, computer operations, computer programs, computer services, or computer software or to create any liability by reason of terms or conditions adopted by, or technical measures implemented by, a Virginia-based electronic mail service provider to prevent the transmission of unsolicited electronic mail in violation of this article. Nothing in this section shall be construed to prohibit the monitoring of computer usage of, the otherwise lawful copying of data of, or the denial of computer or Internet access to a minor by a parent or legal guardian of the minor.[215]

"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 identifying information, as defined in clauses (iii) through (xiii) of subsection C of § 18.2-186.3, 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 1 misdemeanor.

C. Any person who violates this section after having been previously convicted of a violation of this section or any substantially similar laws of any other state or of the United States is guilty of a Class 6 felony.

D. Any person who violates this section and sells or distributes such information to another is guilty of a Class 6 felony.

E. Any person who violates this section and uses such information in the commission of another crime is guilty of a Class 6 felony.

F. This section shall not apply to any person collecting information that is reasonably needed to (i) protect the security of a computer, computer service, or computer business, or to facilitate diagnostics or repair in connection with such computer, computer service, or computer business or (ii) determine whether the

---

[215] *Id.* § 18.2-152.4.

> computer user is licensed or authorized to use specific computer software or a specific computer service.[216]

"Theft of computer services" is defined as follows:

> Any person who willfully obtains computer services without authority, is guilty of the crime of theft of computer services, which shall be punishable as a Class 1 misdemeanor. If the theft of computer services is valued at $2,500 or more, he is guilty of a Class 6 felony.[217]

"Personal trespass by computer" is defined as follows:

> A. A person is guilty of the crime of personal trespass by computer when he uses a computer or computer network 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 6 felony.[218]

Persons injured by violations of the Virginia Computer Crimes Act can also recover damages, including lost profits, and the "costs of suit."[219]

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*** and in such a way as to protect the privacy of nonparties who complain about violations of this section.[220]

---

[216] *Id.* § 18.2-152.5.

[217] *Id.* § 18.2-152.6.

[218] *Id.* § 18.2-152.7.

[219] *Id.* § 18.2-152.12.

[220] *Id.* § 18.2-152.12(D) (emphasis added); *UPS v. Matuszek*, Case No. 1:97-cv-00744 (E.D. Va. 1997) (hacking to reconstruct competitor's customer list).

Similarly, every federal court "has supervisory power over its own records and files."[221]

3. Federal Electronic Communications Privacy Act

The provisions of the Federal Electronic Communications Privacy Act (the "ECPA") known as the Wiretap Act address interception of communications, as follows:

> (a) Offense. Except as provided in subsection (c) of this section whoever—
>
> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
>
> (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.[222]

The provisions of the ECPA known as the Stored Communications Act address dissemination or review of stored communications, as follows:

> (a) Prohibitions. Except as provided in subsection (b)—
>
> (1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and
>
> (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—
>
> (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; and
>
> (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such

---

[221] *Nixon v. Warner Commc'ns, Inc.*, 435 U.S. 589, 598 (1978).

[222] 18 U.S.C. § 2701.

communications for purposes of providing any services other than storage or computer processing.[223]

Civil remedies for violation of the ECPA include injunctive and declaratory relief, actual damages plus the violator's profits in an amount not less than $1,000, and reasonable attorneys' fees and litigation costs.[224] Many states have enacted statutory counterparts to the ECPA.

VII. PRE-INCIDENT RISK MITIGATION

Pre-incident risk management remains a critical component of any franchise system's effort to thwart data security breaches. From the perspective of third party data, there is an affirmative obligation to keep the data safe and secure. Failure to do so can cost the franchise system time, money, and damage to its reputation and goodwill. From the perspective of trade secrets and confidential information, the franchise system has a strong incentive to keep these assets safe and secure to maintain its competitive advantage in the marketplace.

Quoting a "private security expert," former Attorney General Eric Holder once famously said during a trade secret strategy rollout, "there are only 'two categories' of companies affected by trade secret theft -- 'those that know they've been compromised and those that don't know it yet.'"[225] This is an objectively ominous and deflating quote. If the release of trade secrets and proprietary information is inevitable, then is there any utility in attempting to secure its confidentiality? The answer of course is yes—for the myriad reasons described throughout this paper. Safeguarding trade secrets and confidential information not only reduces the risk of costly misappropriation or breaches that can do irreparable damage to a franchise system, but also provides evidence that franchisors made "reasonable efforts" to safeguard the franchise systems as required under law to establish a protectable trade secret and proprietary confidential information.

This next section will provide a roadmap to franchise systems seeking to mitigate potential exposure for trade secret and confidential information theft, misuse, and inadvertent disclosure and for maintaining the safety of third party data in the event of a data breach incident.

A. Update Written Policies and Contractual Provisions

While the scope of what constitutes "trade secrets" and "confidential information" may appear painfully obvious and instinctual to a seasoned franchise practitioner, it may not be to a less savvy franchisee or employee layperson. Franchisees along with employees, contractors, business associates, and partners of franchisors and franchisees may honestly be unaware of the expansive scope of trade secrets and confidential information requiring protection in a franchise system. Therefore, the first line of defense in mitigating the risk of breach is ensuring that all written policies are (1) expansive and adequately descriptive enough to encompass all forms of potential confidential and proprietary information; and (2) easy and straightforward so

---

[223] 18 U.S.C. § 2702.

[224] 18 U.S.C. § 2707.

[225] Attorney General Eric Holder Speaks at the Administration Trade Secret Strategy Rollout, JUSTICE NEWS (February 20, 2013), available at https://www.justice.gov/opa/speech/attorney-general-eric-holder-speaks-administration-trade-secret-strategy-rollout.

bound parties have a clear roadmap to understand their obligations, responsibilities and the role they play in trade secret protection.

A franchise system should continuously examine its exposures based on the various parties it wishes to bind and then update and/or implement policies. These parties include: (1) the franchisor's employees; (2) franchisees; and (3) suppliers, vendors, and independent contractors.

1. Franchisor Employees.

a. Limiting and Prohibiting Risky Employee Conduct

A franchisor should never disregard its own employee practices when it comes to protecting third party data and trade secrets. The responsibilities fall on both the employer and the employee. Franchisors often fail to educate employees about the wide range of confidential information they must safeguard and protect. Employees are also blissfully unaware of the type of risky behavior that can expose the franchise system's trade secrets and other confidential data to a potential breach. The unfortunate reality is that employees often consider the software and technology available outside a business organization as faster, more efficient, and easier to use. This results in employees going outside an employer's informational technology system to communicate with customers and business associates, store data, and conduct other work tasks. The problem is that these resources are often unsecure and untested. As a result, franchisors should enforce written policies prohibiting employees from engaging in these types of unsafe behavior:

(1) using commercial email (*e.g.*, Gmail) for work-related tasks;
(2) posting files online because of email attachment size limitations;
(3) forwarding all work email to a commercial account because of an email retention policy;
(4) using i-phones or other devices for work tasks without the password protection enabled;
(5) using peer-to-peer file sharing services;
(6) working on company materials on home computers;
(7) uploading franchise system confidential and proprietary trade secrets into the cloud or
(8) copying sensitive information to unprotected, portable devices ("thumb" or "jump" drives).

Employees in the workplace are increasingly using cloud technology for work and personal reasons. There are many reasons for a franchise system to prohibit this practice. If the employee departs the franchise system and joins a competing franchise brand, then the employee may continue to have "cloud access" to highly sensitive trade secrets and third party data that he or she uploaded during his or her employment. There are new cases every day showing the risk of cloud usage. In *Zynga Inc. v. Patmore*, a departing employee uploaded 834 sensitive company files to Dropbox, quit his job, and then downloaded them onto a laptop owned by his new employer, which was a direct competitor.[226] Under such circumstances, the franchise system is forced to scramble to determine how much of a breach occurred and how to get its confidential

[226] *Zynga Inc. v. Patmore*, Case 12-525099 (Cal. Super. 2012).

information back. Consider the case of *Integral Development Corp. v. Tolat*, where the District Court of Northern District of California ordered that the employee, Mr. Viral Tolat, return all confidential information of his former employer, Integral Development Corp., that he downloaded onto his Dropbox account.[227] The court also established procedures to verify that Mr. Tolat no longer had Integral's confidential information.[228] In an effort to reconstruct a forensic evaluation of what exactly the former employee did with Integral's confidential information, Integral issued a subpoena to Dropbox requesting "all documents uploaded to, downloaded from, or accessed and viewed" from the employee's Dropbox account.[229] A discovery dispute arose when Dropbox resisted providing all of the requested information, citing the Electronic Communications Privacy Act.[230] The court ruled that the content information would be produced to the independent expert, and not to Integral directly, to address the privacy concerns.[231] While Integral was able to retrieve the information it needed for its forensic investigation, franchise systems should not discount the time and expense incurred by the former employer.[232] In addition to the practical problem of figuring out how to regain control of the trade secrets, the breach could be used as evidence that a franchise system failed to take "reasonable measures" to protect its trade secrets.

The use of public cloud storage exposes vulnerabilities in not just those the franchise system knows but also those it does not know. Public cloud usage can make a franchise system's private data vulnerable to unknown cyber hackers and bad actors. There is a shift among businesses to move data from public systems to private cloud systems, VPNs, and private networks.

International franchise systems are exposed to additional risk. If a franchise system employs staff that travel abroad, then it is prudent for franchisors to be aware of the significant risks associated with foreign travel with laptops and personal digital assistants ("PDAs"). It may come as a surprise to some employers that United States Customs and Border Protection ("CBP") does not need reasonable suspicion to conduct "basic searches" of laptops, PDAs, and storage media (viewing photos and messages and physically examining the device).[233] While the risk of being searched by the CBP is low, employees storing sensitive and confidential information should be aware of the risk and consider taking precautions.[234] Many of these precautions may be burdensome and not administratively feasible but are worth consideration and include:

---

[227] *Integral Dev. Corp. v. Tolat*, No. C 12-06575 JSW (LB), 2013 WL 2389691 at *1 (N.D. Cal. May 30, 2013).

[228] *Id.* at *1.

[229] *Id.*

[230] 18 U.S.C. § 2703.

[231] *Integral Dev. Corp.* 2013 WL 2389691 at *2.

[232] *Id.*

[233] U.S. CUSTOMS AND BORDER PROTECTION, CBP Directive No. 3340-049A, *Border Search of Electronic Devices*, January 4, 2018, available at https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf.

[234] Electronic searches of travelers leaving or entering the U.S. increased more than 50% last year, but the total still remains a small fraction of the overall number of travelers.

1. using temporary or travel devices (phones, laptops or tablets) that do not contain access to trade secrets, confidential or proprietary information;
2. backing up and deleting sensitive data before reaching an inspection point;
3. using a separate user account and/or e-mail account for sensitive information and removing the accounts from device in advance of reaching an inspection point;
4. using strong encryption and complex passwords;
5. using two-factor authentication; and
6. partitioning and encrypting hard drives.

Searches are limited to information that is stored on the devices so information accessible through the cloud is not searchable. Travelers are not required to turn over passcodes and passwords. However, a failure to do so could result in confiscation of the devices for an "advanced search." Reports are surfacing of these devices either never being returned, or being returned damaged, tampered with, and (certainly) accessed by unknown persons.

b. The Employee Handbook

Curbing problematic employee behavior is not the only step a franchise system should take to protect its trade secrets and confidential information and third party data. A franchisor's employee handbook should have as fulsome a confidentiality section as the franchisor's operations manual with its franchisees. Employer policies should prohibit employees from downloading, duplicating, altering, removing, deleting or installing data, files, passwords, and programs without prior written authorization from the individual(s) or committee in charge of information security (or a high-level administrator and/or executive depending on the personnel employed by the company).

The handbook should include a strong password policy for all employees that requires combinations of numbers, letters and symbols of several characters in length. A common recommendation provided by privacy industry professionals is stringing together four completely unrelated words (for example, *DogDrinkSummerThumb*). Employees must be prohibited from sharing accounts or passwords. Because employers often keep confidential information in a computer program or system, there must be a method to ensure that only authorized employees will have access to it to maintain secrecy. Individualized and unique login credentials act as a means of identity verification so that only those employees who are meant to access confidential information can do so. The use of unique individualized credentials to access to proprietary information is both a recommended risk management technique and can also act as evidence to establish the materials constitute "trade secrets."[235]

The strength of a franchise system's social media also plays a role in protecting trade secrets and confidential information. For example, the social media policy should have guidelines for safe blogging and posting on the Internet. Franchisors must caution employees about disclosing too much information online to prevent unintentional disclosure, which could jeopardize

---

[235] *See Arminius Schleifmittel GmbH v. Design Indus. Inc.,* No. 1:06CV00644, 2007 WL 534573 (M.D.N.C. Feb. 15, 2007). In *Arminius*, a company alleged that its former employee misappropriated its electronic library containing precise specifications for how to manufacture proprietary sanding tools for each of their individual customers' designs. Id. at *3. In determining that the library constituted traded secrets, the court noted that the library was only accessible to certain employees who hold a unique login and pass-code. Id.

trade secret and confidential information protection. Even linking to customers on LinkedIn may inadvertently disclose customer lists.

A few states have recognized a cause of action under a *respondeat superior* or vicarious liability theory for employers hiring a new employee who stole trade secrets from his or her previous employer.[236] To avoid potential vicarious liability for a new employee's misappropriation of a former employer's trade secrets, new employees (especially new employees hired for c-suite level executive roles) should acknowledge and agree:

(1) the employee is not subject to any agreement with his or her prior employer or any other third party that would affect the employee's right to perform the services he or she was hired by the franchisor to provide;
(2) the employee has not disclosed any trade secrets or confidential or proprietary information of any former employer or third party to the franchisor;
(3) the franchisor has instructed the employee not to bring, use, or disclose any trade secrets or confidential or proprietary information of any former employer or third party to the franchisor; and
(4) the employee will not use during his or her employee any trade secrets or confidential or proprietary information of any former employer or third party.

Employees should be required to sign an acknowledgement of their receipt of the handbook or policy, and the acknowledgement should set forth the employee's agreement to be bound by the policy. Policies are an important step in maintaining the secrecy of confidential information because they may constitute notice to employees. Indeed, courts have denied affording trade secret protection to employers that failed to have written policies governing confidentiality and trade secrets.[237]

Large franchise systems should also consider establishing an "employee tip line" to encourage notification where employees can report breaches.

2. Franchisees

There are primarily three avenues for franchisors to use when attempting to avoid data breaches and mitigate loss in the event of a data breach at the franchisee level: (i) the franchise agreement; (ii) the operations manual; and (iii) franchisee training.

a. Franchise Agreement

A franchise system should review its franchise agreement, focusing particular attention on the following:

---

[236] *See, e.g., Newport News Indus. v. Dynamic Testing Inc.*, 130 F. Supp. 2d 745, 754 (E.D. Va. 2001).

[237] *See CMBB LLC v. Lockwood Mfg. Inc.*, 628 F. Supp. 2d 881 (N.D. Ill. 2009). In *CMBB*, a former employee was permitted to retain her laptop with access to her former employer's (CMBB) customer names, contacts, telephone numbers, product purchases, pricing and amounts paid. Id. at 885. The court granted summary judgment to the employee in CMBB's misappropriation case finding that CMBB did not take the necessary steps to protect the customer information as a trade secret. For example, CMBB did not tell the employees that the information was confidential or safeguard the information under any established policies or procedures. Id.

i. Definition of "Intellectual Property". The franchise agreement's definition of "intellectual property" should include an express description of all potential trade secrets, including product recipes, formulas, techniques, test records, source code, architectural blueprints of franchise units layouts, quality control data, sales forecasts, and strategic business plans. The definition should be broad but also tailored to the specific property that the system considers "trade secrets."[238] The definition should be reviewed and revised, when necessary, each year as part of the annual FDD updating process.

ii. Confidentiality. A franchise system should always require that a franchisee limit access to trade secrets and confidential information to those with a "need to know." A franchisee should understand that not every employee and contractor should have access to the operations manual, recipes, customer lists, product formulas, and marketing and business strategies. Limiting access to confidential information is the easiest way to decrease the likelihood of such data being disclosed. The confidentiality provision should clearly outline how and when in those limited circumstances confidential information may be disclosed to third parties.

iii. Indemnification. Franchisors will want to examine their franchise agreement's indemnification provisions, particularly as to damages resulting from data breaches that are caused due to the actions or inactions of the franchisee. Franchisors should ensure that such risk is allocated to the franchisee.

iv. Insurance. A review of the franchise agreement's insurance obligations should include updating insurance coverage to cover losses due to a data breach. As described in more detail in this paper, losses resulting from data breaches involving confidential information, like protected health information (PHI) and personally-identifiable information (PII) and credit card information of employees or customers, are likely covered under a good cyber liability policy. However, monetary losses suffered by a franchisor in the event of an unauthorized release or theft of trade secrets are typically not insurable at a reasonable cost.

v. Duties of Franchisee. The franchise agreement should require each franchisee to adopt its own data security policy and response plan. This plan should address responding to breaches of PHI, PII, and credit card data as well as trade secrets and other proprietary information. It is likely that the components of the response plan adopted by a franchisee will largely be developed from samples provided by the franchisor. Franchisors should demand franchisees be PCI compliant. Franchisors should also require that a franchisee's information security program and policy include an obligation to cooperate and to promptly and fully communicate with the

---

[238] *Dippin' Dots, Inc. v. Frosty Bites Distribution, LLC*, 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).

franchisor in the event of a breach.[239] Franchisors also want to ensure cooperation by requiring franchisees to abide by any request from the franchisor necessary to allow the franchisor to comply with data privacy laws applicable to the franchise system regarding processing, storage, handling, collection, use, transfer, and transmission of customer data.

vi. Definition of "Customer Data". Franchisees may have an incorrect narrow view of what constitutes "personally identifiable information" and other protectable third party data under the law. They may believe it includes only social security numbers and detailed biographical information. However, the definition is much broader under most state laws. Many (if not most) franchise agreements now require franchisees to safeguard and comply with all applicable laws, regulations, and industry best practices regarding PHI, PII, and other third party data but may not define that information broadly and clearly enough. Make sure that any definition of "customer data" includes any information on customers that identifies or can be used to identify, contact, or locate or be traced back to a specific person to whom such information pertains, or from which identification or contact information of an individual person can be derived, including but not limited to PII.

vii. Alternative Dispute Resolution. Franchise agreements and other agreements containing non-disclosure and confidentiality provisions should carve out the franchisor's right to enforce its intellectual property through the court system from any alternative dispute resolution procedures (like mediation or arbitration).

The existence of strong and fulsome contractual provisions is useful not just to mitigate a breach but also to better position the franchise system if a breach does occur. Misappropriation of trade secrets is a tort claim arising under common law or by statute. Therefore, a franchise system can assert the claim even in the absence of a written agreement. However, the existence of a right under the franchise agreement will provide the franchisor with a breach of contract claim as well arising from the improper use or disclosure of information. 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."[240] In the case of a data breach involving third party data or PII, these contract provisions can help shift liability to the franchisee where the franchisee breached its obligations to maintain the safety and security of customer data, including PII, PHI, and credit card information.

---

[239] *See* Len McPhee, Paul Reeve, Shelly O'Callaghan, and Sally King, *Data Privacy and Security: Can any Brand Sleep at Night*, IFA 48th Annual Legal Symposium, at 27 (2015).

[240] *See* Michael J. Lockerby, James P. Mittenthal, and Heather Carson Perkins, *Protection of Franchise System Trade Secrets and Confidential Information, and Enforcement of Non-Disclosure Agreements, In the Digital Age*, ABA *35th Annual Forum on Franchising,* W-3 at 23 (2012).

b. Operations Manuals

As described in the employee section of this paper, it is recommended that a franchise system encourage franchisees to limit those employees who have access to third party data, confidential information, and proprietary trade secrets. To the extent reasonable, franchisees should take the same precautions and preventive measures taken by the franchisor. Most franchise systems now provide their operations manuals and other training materials online. The franchisor should use a private network-encryption program, secure passwords, on-screen confidentiality warnings, and bold "Confidential" boxes around confidential information.[241]

c. Initial and Ongoing Training

There are two competing forces related to training franchisees. It is understandable that franchisors are intuitively averse to involving themselves in the daily business operations of the franchisee units due to the increased risk of vicarious liability claims and joint employer issues. However, the financial impact on a franchise system in the event of a unauthorized disclosure of a trade secret or data breach releasing trade secrets or other confidential information likely warrants providing additional guidance to franchise units. For example, there are third party service providers that can provide day to day tips for maintaining proper data security compliance procedures and provide general information about a business's obligations. Data security training is often focused on PCI-DSS compliance and the safeguarding of employee and customer data. This is especially important in the context of fast casual concepts, restaurants, and retail based franchise systems as breaches to a franchisee's POS system can expose not just the franchisee's customer data but also customer data of other franchisees and company owned outlets. In such cases, implementing and communicating system-wide standards and procedures to franchisees may not only limit the likelihood of a breach but may also limit the scope of enforcement by authorities.[242]

Comprehensive training on best practices in safeguarding confidential information can and should include trade secret protection. Further, franchise systems should conduct regular audit and compliance checks in the same manner that a system conducts quality control checks on a franchisee's services and products. Regular communication, ongoing training, and auditing for compliance may be helpful for avoiding data breaches at the franchisee level.

3. Suppliers and Independent Contractors

There are a number of steps that a franchise system can take to protect its trade secrets, data, and confidential information from breach, theft, or misuse at the supplier, vendor, and independent contractor level. First, conduct a risk assessment and evaluate factors like:

1. type of data being shared (trade secrets, other confidential franchise system information, customer or employee PHI, PII or credit card information)
2. how many records are involved;

---

[241] *PartyLite Gifts, Inc. v. MacMillan*, No. 8:10-CV-1490-T-27EAJ, 2010 U.S. Dist. LEXIS 133440, at *10 (M.D. Fla. Nov. 24, 2010).

[242] *See* JoAnn Carlton, Heather Enlow-Novitsky, and Matthew Fore, *Data Security and Addressing the Risk in the Franchise System*, IFA 51st Annual Legal Symposium, at 32 (2018).

3. value of the contract; and
4. financial strength of vendor to meet indemnity obligations.

Then conduct due diligence on vendors' cybersecurity practices. The extent of this due diligence review should correlate to the volume, sensitivity, and type of proprietary and confidential information that will be shared. Prepare a form of privacy and security questionnaire and require that every prospective supplier and vendor complete one prior to engagement. It is critical to conduct a certain amount of due diligence on all types of vendors—not just those that the franchise system immediately considers applicable. For example, custodial staff may have access to sensitive confidential information in tangible written form. A franchise system should consider the following provisions when entering into a contract with an independent contractor, supplier, or vendor:

1. Reserving the right to audit the cybersecurity practices of the vendor to confirm that the vendor is complying with its obligations under the agreements and under law;
2. Requiring compliance with all laws and industry standards regarding the use, storage, and disclosure of sensitive and confidential information;
3. Requiring indemnification for failing to maintain appropriate security measures and set minimum insurance limits[243];
4. Responding to contract provisions whereby suppliers and vendors seek to impose limitations (or caps) on liability and disclaimer of damages on the amount and type of losses recoverable by a customer by carving out any disclaimer of damages and limitations on liability for data breaches or breaches of the non-disclosure and confidentiality provisions of the contract;
5. Requiring notification of a vendor data breach involving any of the franchise system's data, confidential information, or trade secrets, and obligating the independent contractor, supplier, or vendor to cooperate during an investigation.

To avoid potential vicarious liability claims by other franchise systems or businesses with whom your independent contractors are engaged, ensure that there is a written agreement between the parties confirming the independent contractor's status and affirmatively stating that the franchisor has no right to control its work. In *Ennis Transportation Co. Inc. v. Richter*,[244] a number of employees left a transportation company and formed a competing company. The former employer then brought a lawsuit against the former employees and one of the former employees' new client under a vicarious liability theory allegedly that the parties were misappropriating confidential customer lists and other information obtained during the course of their employment.[245] The court granted summary judgment to the company client in part because

---

[243] For a more detailed description of insurance, *see* Section IV of this paper.

[244] No. 3:08-CV-2206, (N.D. Tex. Aug. 22, 2011).

[245] *Id.*

it found that the agreement between the client and former employees clearly established an independent contractor relationship and the client had no right to control its work.[246]

B. Implement Physical and Electronic Security Measures

The implementation of proper physical and electronic security measures is a critical component of any risk mitigation plan. These are common sense, and often inexpensive, recommendations. Problems often arise, however, when franchise systems are inconsistent in enforcing the policies with employees who may not want to be bothered with changing the way they operate on a day-to-day basis. The below best practices are reasonable and reduce the risk of data breaches when enforced on a regular and consistent basis.

1. Shred, Destroy, and Purge!

To ensure the safety of trade secrets and third party data, implement document-shredding procedures and encourage system franchisees (for example, during initial or periodic training or via the operations manual) to implement document shredding procedures. Sensational news stories constantly bombard us with stories of sophisticated computer hackers and thieving employees. Many security risks, however, result from businesses' own sloppy physical security measures. Trash cans get knocked over outside and dumpsters get ransacked. Remind those with access to trade secrets to shred any documents containing or referencing such trade secrets. Provide shredding receptacles throughout offices and encourage franchisees to maintain clearly labeled shredding receptacles at each unit location. Periodically remind employees and franchisees that placing confidential documents in standard trash cans is not a secure disposal system. Protection of trade secrets contained in paper form is still important even in the digital age. Access to this information must be secured against threats from visitors to the business, including cleaning staff, security guards, and former employees who still have access.

In addition, it is important to have detailed document management and retention policies in place. No business needs to retain every email ever dispatched or received.

2. Control Over Access

One of the most obvious but often overlooked steps a franchise system can take to minimize its risk for data breaches is to limit the parties with access to the information in the first place. Confidential information, especially highly sensitive trade secrets, should be distributed on a "need to know" basis. Are employees limited to having access to only the confidential information necessary to provide the services they were hired to perform? Does the headquarters maintain a log of all visitors? Are guests provided badges and monitored? Are employees encouraged to pick up print jobs from copiers immediately, or can they linger in a mail room or common area of the office? If information is confidential, then make sure it is marked as such.[247]

---

[246] *Id.*

[247] *See CMBB LLC v. Lockwood Mfg. Inc.*, 628 F. Supp. 2d at 885 (citing the failure of a company to mark hard copies of customer information to indicate that they were considered confidential or a trade secret as evidence that the company did not take the necessary steps to protect the customer information as a trade secret).

Password protect sensitive electronic files and servers.[248] Use sign-on screens on computers that does not allow user to proceed without agreeing that the material to be viewed is confidential, *e.g.*:

> WARNING: The information on FRANCHISOR'S system is confidential and proprietary. Unauthorized use, duplication, transmittal or disclosure of this information is strictly prohibited. System activity is monitored and recorded.

Put employees on notice that they have no expectation of privacy in connection with any uses of company equipment. Ensure that there are locks on file cabinets and file rooms and otherwise store trade secrets in a restricted access area. Install security cameras where appropriate. To the extent possible, prohibit employees from removing highly sensitive information from headquarters.

3. Electronic Security Measures

A franchise system can take its own steps to thwart this behavior by (1) preventing access to external web-based e-mail services like *Gmail* from company servers and having other technological blocks in place to prevent installation or downloading of unnecessary or unwanted software or programs and physically blocking certain web sites (or all web sites that are not work related);[249] (2) encrypting highly-sensitive electronic documents and preventing them from being forwarded to unauthorized users; (3) disabling or eliminating USB ports on all but certain designated company computers; (4) moving the "reply all" button on company email to a less accessible position on the screen; and (5) using programs that strip out track changes and metadata when documents are emailed. Remind employees to use care when working on laptops and other digital storage devices off-site to prevent third parties from seeing their screen or purchase physical "privacy screens".

4. Prepare for Attacks from the Outside

A franchise system must also properly secure its system from outside attacks, especially attacks that seek to steal third party data. Having a firewall is not sufficient. A franchise system may consider having a redundant firewall where extremely sensitive information is stored. Regularly change passwords on firewalls and any wireless network. Ensure that IT or IS staff regulatory evaluate existing firewalls, antivirus software, and other security measures applicable to the franchise system's computer systems and Internet connections and makes necessary upgrades on a regular basis. Have an intrusion detection system managed and monitored by a provider to discover malware that be attempting to infect the system. Only permit downloading of applications deemed secure. Monitor reported security risks, breaches, and attempts at breaches (even unsuccessful attempts) and make those adjustments to the franchise security system as appropriate. Conduct penetration tests to determine whether employees are susceptible to

---

[248] *AutoNation Inc. v. Peters*, No. 16-60010-CIV-COHN/SELTZER, 2016 U.S. Dist. LEXIS 57373, at *11 (S.D. Fla. April 29, 2016). In *AutoNation*, the departing employee obtained confidential and proprietary information through a password protected database and specialized, private training accessible only to designated personnel. Id. at *2.

[249] *See* Michael J. Lockerby, James P. Mittenthal, and Heather Carson Perkins, *Protection of Franchise System Trade Secrets and Confidential Information, and Enforcement of Non-Disclosure Agreements, In the Digital Age*, ABA 35th Annual Forum on Franchising, W-3 at 22-23 (2012).

spearphishing or social engineering attacks. These schemes deceive victims (typically employees) into voluntarily transferring funds or divulging confidential information (like tax returns, employee W-2s, and customer and employee information). A franchise system may be surprised by how easily employees turn over information and passwords based on requests from a targeted email.

5. Pre-Departure Investigations

If a franchisor has a reasonable belief that a franchisee is choosing not to renew its franchise agreement or an employee is departing under suspicious circumstances, or if there is other reason to suspect possible misappropriation of trade secrets, the franchisor should preserve records of the employee's computer activity in the weeks or days leading up to the departure of the franchisee or employee. For example, in the case of employees, a franchisor may create copies of emails or forensic images of hard drives. Similarly, in the case of a franchisee, the franchisor can use its authority under the franchise agreement to independently access the franchisee's electronic data and check computer systems for unusual copying and downloading.[250] Doing so may lead to crucial evidence of abnormal computer activity used in future litigation over trade secret misappropriation.[251] It is becoming more and more common for an employer to find a former employee transferring company confidential information to thumb drives, external hard drives, or other devices.[252] If any employee in a sensitive position is going to work in a similar or related industry, accept the resignation immediately and terminate the employment as soon as possible. If the employee is allowed to continue working for any time after giving notice, monitor electronic mail access and building access logs to determine if the employee is coming to the facility at odd times or has been staying in the facility for unusually extended periods of time.

C. Conduct Exit Interviews with Departing Franchisees, Employees, and Contractors

The first step in mitigating a franchisor's risk from theft or misuse by a former employee is to immediately terminate the employee's access to sensitive materials.[253] Franchisors should conduct an exit interview with every departing employee. While a departing employee is unlikely to readily admit that he or she intends to misappropriate the trade secrets of the franchise system for personal advantage (or the advantage of a future employer), the exit interview serves many

---

[250] *See LeJeune v. Coin Acceptors Inc.*, 381 Md. 288, 314, 849 A.2d 451 (Md. 2004) (employee misappropriated his employer's trade secret when, on the last day of his employment, he transferred confidential information from his work laptop to a CD that he intended to keep for his personal use).

[251] Peter A. Steinmeyer, *Preventing the Misappropriation of Trade Secrets Through Proactive Policies and Procedures, as appeared in Labor and Employment Law*, Labor & Employment Law Illinois State Bar Association Newsletter, May 12, 2009, available at https://www.ebglaw.com/news/preventing-the-misappropriation-of-trade-secrets-through-proactive-policies-and-procedures-as-appeared-in-labor-and-employment-law/.

[252] *See Integral Dev. Corp.*, No. C-12-06575, 2013 WL 2389691 (N.D. Cal. May 30, 2013).

[253] Failing to have proper protocols in place for departing employees is not only bad risk management but also jeopardizes the franchisor's ability to succeed on future claims against an employee. *See CMBB LLC v. Lockwood Mfg. Inc.*, 628 F. Supp. 2d at 885 (citing the failure of a company to implement any written policy or procedure as to what a former employee was to do with customer information after leaving employment and the fact she was permitted to retain an "unscrubbed" company laptop as evidence that the company did not treat such information as confidential or a trade secret).

purposes. An exit interview helps a franchisor or franchisee understand what access the employee had to confidential information and trade secrets and places the departing employee on notice of its post-term nondisclosure obligations. Some companies even use a human resource manager or other neutral unassuming representative to encourage the departing employee to let his or her guard down and provide honest and candid responses.

At the exit interview, it is helpful to have a checklist of information to review and questions to ask the employee. The checklist should include:

1. Receiving confirmation that the employee does not possess any confidential information. Ask the departing employee detailed questions to prompt his or her memory and elicit a complete and accurate response
   a. "Have you stored any company documents in the cloud?"
   b. "Do you have any company data or materials at home?"
   c. "Have you emailed any company data to a personal email?"
   d. "Have you returned all intangible and tangible copies of the franchise system's property containing company information (devices, external drives, passwords, paper and electronic documents and files)?"
   e. Have you returned access card, id-badges, credit cards, keys, computer or other devices provided by the company?"
2. Obtaining a signed certification, where possible, that the departing employee did return all company data.
3. Providing a copy of the employee's confidentiality agreement and reminding the departing employee of his or her ongoing obligation to maintain the confidentiality of trade secrets and other confidential information.
4. Explaining that the non-disclosure obligations remain in effect although the employment relationship is terminated.

Interview remaining employees to see if they know anything, and have the employee's immediate manager confirm whether the individual should or should not have in his or her possession and can be sure that everything is accounted for and physically review the work area. Disable access to voicemail, electronic mail, computers, and other information and materials. Do not wipe the hard drive of any workstation, desktop, or laptop returned to company's inventory without checking for evidence of misappropriation and making sure that all files on the hard drive that need to be kept have been appropriately archived. Check email history for evidence of emails to a home email address or to a new employer. Keep abreast of former employees' activities in the industry for a number of months after departure. A former employee may not start to engage in competitive activity that could misappropriate trade secrets for a number of months after leaving the franchise system.

A franchisor may also consider providing a sample checklist for its franchisees at initial training or as part of the operations manual. The franchisee can use the sample checklist for its own departing employees who had access to the franchise system's trade secrets or third party data or attended the franchisor's training.

1. Keep Yourself in the Know

In addition to educating franchisees, employees, and contractors about the scope of the franchise system's trade secrets but the franchisor should also be diligently aware of (i) the scope

and extent of its trove of trade secrets, confidential and sensitive information and (ii) how such information is gathered, stored, used and eventually destroyed or deleted.

A franchise system should periodically inventory its trade secrets and identify all trade secrets by type, value to the franchise system, location, and storage method. Listing a system's trade secrets in details reminds a franchisor of the scope of information that it must protect and trigger new thoughts and ideas on protecting such data. As the portfolio of a franchise system's trade secrets is constantly changing, the exercise should be taken at least on an annual basis.

Implement a trade secrets policy and appoint a Chief Privacy Officer, Trade Secrets Compliance Officer, or similar executive position. This person should be responsible for overseeing the execution of all non-disclosure agreements, maintaining a log of all non-disclosure agreements in place, and monitoring steps taken to maintain the secrecy of trade secrets and confidential information. Conduct audits to make sure that all required protocols are being followed. Implement appropriate sanctions in response to discovered noncompliance and incorporate trade secret and data privacy compliance into compensation decisions.

Understand how data is being collected and stored. For example, digital copiers expose businesses to the same cybersecurity risk as associated with computers since they have hard drives storing sensitive data and run on smart technology. Franchisors should ensure that all equipment and technology that may store trade secrets or confidential information have updated safety and security features. The Federal Trade Commission's Digital Copier Data Security: A Guide for Businesses provides best practices for integrating copiers safety and securely into a businesses' informational system.[254]

VII. CONCLUSION

Hindsight is obviously 20-20, and what seem to be "best practices" today may not prove to be so good after all following a cyberattack of unprecedented scope or methodology. The time to develop and implement plans for responding to a breach (and hopefully avoiding a breach in the first place) is long before it occurs, not after the fact. Hopefully this paper will help franchise systems have the right procedures in place when a breach occurs so that the focus can be on implementing a swift and sure response rather than wasting valuable time figuring out what to do.

---

[254] FEDERAL TRADE COMMISSION, Digital Copier Data Security: A Guide for Businesses, July 2017, available at https://www.ftc.gov/tips-advice/business-center/guidance/digital-copier-data-security-guide-businesses.

BIOGRAPHIES

Jason Adler is General Counsel and Secretary for Cellairis Franchise, Inc. located in Alpharetta, Georgia. Cellairis and its affiliates are manufacturers and distributors of accessories for wireless devices and currently operate units domestically and internationally in 8 countries, as well as holding retail space within numerous retail centers, such as Walmart. Mr. Adler is responsible for handling all legal matters for Cellairis and its affiliates, which cover a wide range of legal and business issues including franchise (registration and system compliance), litigation matters, corporate governance and regulatory matters, intellectual property, real estate, labor and employment, celebrity and endorsement law, and social media/information technology matters, insurance/risk management, and mergers and acquisitions both in domestic and international forums. With respect to franchising matters, Mr. Adler handles compliance with state and federal regulations including drafting franchise disclosure documents, complying with state franchise registration and disclosure laws, preparing expansion into international markets, and developing social media policies, operational standards, and advertising guidelines.

Mr. Adler co-presented at the 39th Annual Forum on Franchising, in Miami, Florida on "Right of Publicity Claims in a Digital Age". Mr. Adler also co-authored an article entitled "Dine and Dash Arbitration Style" published in the Spring 2017 issue of The Franchise Lawyer and he also co-authored an article entitled "Critical Privacy and Data Security Risk Management Issues for the Franchisor" published in the Summer 2015 issue of the Franchise Law Journal. Additionally, Mr. Adler is a frequent presenter and author on domestic and international franchise-related topics, including privacy and information security loss prevention, best practices for domestic franchisors expanding internationally, and the ethical issues that arise for domestic franchise lawyers advising international clients. Mr. Adler currently serves as the Chair for the Corporate Counsel Division for the American Bar Association, Franchising Section, as well as on the Board as immediate Past Chair, for the State Bar of Georgia, Franchise and Distribution Section. Mr. Adler also serves as President for Creating Connected Communities, a 501(c)3 organization, with the mission to provide young adults with tools and resources to assist people in need and to help them become community leaders through partnership, advocacy and mentorship training, where the seminal event each year is Christmas celebration for over 800 children from homeless shelters, foster care homes and refugee centers around metro-Atlanta every December with the help of over 300 teen volunteers. Mr. Adler also serves as Treasurer and advisor to numerous Judges in Atlanta, Georgia, by providing campaign finance advice as well as handling all of the regulatory and compliance requirements promulgated by the Georgia Government Transparency and Campaign Finance Commission.

Mr. Adler received his J.D. degree in 2002 from the Emory University School of Law, where he was the Managing Editor of the Bankruptcy Law Journal. He received a Bachelor of Arts degree majoring in Economics, minoring in Business and Managerial Economics, and receiving a Legal Studies Concentration from Brandeis University in 1999.

Eleanor Vaida Gerhards is a partner at the national law firm of Fox Rothschild LLP. As co-chair of the firm's Franchising, Licensing and Distribution Practice Group, she concentrates her practice on commercial transactions and compliance matters representing primarily franchisors, area developers and master franchisees. She also represents start-up franchisors in the establishment of franchise systems and, as a member of her firm's insurance group and privacy/data security group, she often counsels franchise systems on insurance coverage matters and cyber security issues. Eleanor serves as Chair of the IFA Philadelphia Women's Franchise Network and sits on the ABA Forum on Franchising Program Committee. Eleanor frequently writes and speaks on legal issues in the franchise industry and is a previous presenter at the ABA Forum on Franchising and IFA Legal Symposium. She recently authored a chapter in the ABA book Exemptions and Exclusions under Federal and State Franchise Registration and Disclosure Laws and her articles have appeared in the ABA Forum's Franchise Lawyer newsletter, the Franchise Law Journal, Law360 and Property Casualty 360. Eleanor has been named a "Legal Eagle" by Franchise Times for the last 3 years, a "Rising Star" by Superlawyers, a Pennsylvania "Lawyer on the Fast Track" by the Legal Intelligencer as well as recognized by Who's Who Legal Franchising and named among Philadelphia's Business Journal's 40 under 40.

Michael J. Lockerby is a partner with the law firm of Foley & Lardner LLP, resident in the Washington, D.C. office, and one of the co-chairs of the firm's national Distribution & Franchise Practice Group. For the past 34 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 dealers, distributors, and franchisees. He regularly appears throughout the country in state and federal trial courts and before arbitrators and other ADR providers, including in class actions and system-wide litigation. His recent litigation experience involving misappropriation of trade secrets and cyber breaches includes a successful jury trial in Virginia state court, litigation between two Taiwanese competitors in North Carolina Business Court, litigation against a terminated franchisee in Tennessee in which the federal judge ordered a forensic examination, and an ongoing arbitration in Washington, D.C.

Throughout his career, 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, as Editor-in-Chief of The Trade Secret Handbook: Protecting Your Franchise System's Competitive Advantage, and as a co-author for the trade secret chapter of the Intellectual Property Handbook (2d ed.), a joint project with the ABA Section of Intellectual Property Law.

Mr. Lockerby received a B.A. in 1978 from the University of North Carolina at Chapel Hill and a J.D. in 1984 from the University of Virginia. Between college and law school, he worked as a research assistant for the Joint Economic Committee of the U.S. Congress and as a legislative assistant for the late Senator John Heinz (R-Pennsylvania).