THE SECRETS OF TRADE SECRETS:

PROTECTING YOUR COMPANY'S TRADE SECRETS AND PROTECTING YOUR COMPANY AGAINST TRADE-SECRET CLAIMS

INTRODUCTION

By focusing on the Uniform Trade Secret Act's application in Minnesota, this article provides a highly detailed look at how the Act operates in a real business environment. Although any business should seek legal advice regarding the details of the Act's implementation in that business' particular jurisdiction, this article should help a company spot red flags in its operations.

I. WHY BOTHER?

Knowledge regarding trade-secret law is essential to almost any business. That knowledge can mean the difference between critical business assets being protected or ending up in a competitor's hands. That knowledge may mean the difference between facing a large jury verdict or a quick, favorable resolution to a claim. The first step in analyzing any trade-secret issue is determining whether the information constitutes a trade secret.

II. WHAT IS A TRADE SECRET?

A. INFORMATION COVERED

A wide variety of information potentially qualifies as a trade secret, including formulas, patterns, compilations, programs, devices, methods, techniques and processes.[1] The information must, however, meet an additional three-factor test before it can be considered a trade secret.[2]

First, the information must not be generally known or readily ascertainable.[3] If the information is "available in trade journals, reference books, or published materials," the information is generally known.[4] Where only a small group of people have the ability to design the trade secret and it cannot readily be reverse-engineered, the trade secret is not readily ascertainable.[5] The "requirement for a trade secret that information sought to be protected must not be generally known or readily ascertainable is satisfied if the information is not quickly available through proper means."[6] The fact that some of the information that constitutes the trade secret is in the public realm is not dispositive of whether information constitutes a trade secret.[7] For instance, a compilation of publicly available information may constitute a trade secret if the compilation affords a competitive advantage and is not readily ascertainable.[8]

Second, the information must gain independent economic value from its secrecy.[9] "Generally, if substantial time and money would be required of a competitor to develop the same information, that information has economic value."[10] If introducing the information into the marketplace allows another business to produce a competing product, and if the competition results in lower profit margins, the information derives independent economic value from its secrecy.[11]

---

1 Minn. Stat. § 325C.01 (West 2014).
2 Minn. Stat. § 325C.01; *Electro-Craft Corp. v. Controlled Motion, Inc.*, 332 N.W.2d 890, 899-902 (Minn. 1983).
3 *Electro-Craft*, 332 N.W.2d at 899.
4 *Surgidev Corp. v. Eye Tech., Inc.*, 648 F. Supp. 661, 688 (D. Minn. 1986).
5 *Scott Equip. Co. v. Stedman Mach. Co.*, Civ. No. 06-906 (JNE/JGL), 2003 WL 21804868, at *2 (D. Minn. July 31, 2003).
6 *Surgidev*, 648 F. Supp. at 688 (citing *Electro-Craft*, 332 N.W.2d 890).
7 *Avidair Helicopter Supply, Inc. v. Rolls-Royce Corp.*, 663 F.3d 966, 974 (8th Cir. 2011); *CHS Inc. v. Petronet, LLC*, Civ. No. 10-94 (RHK/FLN), 2011 WL 1885465, at * 8 (D. Minn. May 18, 2011).
8 *Avidair*, 663 F.3d at 972.
9 *Electro-Craft*, 332 N.W.2d at 900.
10 *Surgidev*, 648 F. Supp. at 692.
11 *Wyeth v. Natural Biologics, Inc.*, Civ. No. 98-2469 (JNE/JGL), 2003 WL 22282371, at *19 (D. Minn. Oct. 2, 2003); *I-Sys., Inc. v. Softwares, Inc.*, Civ. No. 02-1951 (JRT/FLN), 2004 WL 742082, at *14 (D. Minn. Mar. 29, 2004).

Third, a plaintiff must show that it made reasonable efforts to maintain the secrecy of the trade secret.[12] Trade secret law "does not require the maintenance of absolute secrecy; only partial secrecy or qualified secrecy has been required under the common law."[13] For instance, a party "acted reasonably to maintain secrecy by requiring a confidentiality agreement from [the defendant] and marking its documents and files as confidential."[14]

PRACTICAL PERSPECTIVE: Evaluating whether information constitutes a trade secret is difficult and experienced counsel is a necessity. From my experience in litigating trade-secret claims, the more technical the information you are seeking to protect, the more likely a jury, judge, or arbitrator is to conclude the information is a trade secret. Thus, the process for coating a medical device will more likely be treated as a trade secret than the business plan for a franchise concept. Moreover, the more specific the information that is sought to be protected, as opposed to more general categories of information, the more likely it is to be protected. Thus, the detailed, relatively unique manual of curriculum to run a swim program is more likely to be protected than the concept of youth-oriented swim lessons. When I evaluate a client's trade-secret claim, I utilize the one-sentence trade-secret test. Basically, I have found that a client that can explain to me their trade secret in one sentence generally has a stronger claim.

B. INFORMATION EXCLUDED

Numerous categories of information have been found not to constitute trade secrets as a matter of law. Generally, less technical information is less likely to be considered to be a trade secret. The following categories of information have been held not to be trade secrets:

1. CUSTOMER LISTS

Although it comes as a surprise to many business people, a company's customer list usually is not a trade secret.[15] The primary reason for denying trade secret status to customer lists is that the identity of customers is readily ascertainable.[16] An underlying rationale is that courts do not want to create backdoor non-competes through the trade secret statute.[17] Additionally, there is a strong public interest in preserving competition.[18]

In some limited circumstances, a customer list might be protected. A customer list that contains more than bare customer names and includes a customer's buying, pricing and payment history may be considered a trade secret.[19] Moreover, if the customer list segregates customers into high-volume or high-margin categories, the list might be protected as a trade secret.[20] Even if the customer list constitutes a trade secret, a party can waive trade secret status by providing a reference list that contains current customers to potential customers.[21] The best way for a business to protect customer information, however, is to enter into a valid non-compete agreement.

12 *Electro-Craft*, 332 N.W.2d at 901.
13 *Surgidev*, 648 F. Supp. at 692-93.
14 *K-Sun Corp. v. Heller Invs., Inc.*, Nos. C4-97-2052, C6-97-2053, 1998 WL 422182, at *3 (Minn. Ct. App. July 28, 1998).
15 *Harley Auto. Group, Inc. v. AP Supply, Inc.*, Civ. No. 12-1110 (DWF/LIB), 2013 WL 6801221, at *7 (D. Minn. Dec. 23, 2013); *Equus Computer Sys. v. N. Computer Sys., Inc.*, Civ. No. 01-657 (DWF/AJB), 2002 WL 1634334, at *4 (D. Minn. July 22, 2002); *Universal Hosp. Servs., Inc. v. Henderson*, Civ. No. 02-951 (RHK/JMM), 2002 WL 1023147, *4 (D. Minn. May 20, 2002); *Newleaf Designs, LLC v. Bestbins Corp.,* 168 F. Supp. 2d 1039, 1044 (D. Minn. 2001) (citing *Lasermaster Corp. v. Sentinel Imaging,* 931 F. Supp. 628, 637-38 (D. Minn. 1996)).
16 *Equus*, 2002 WL 1634334, at *3-4; *Associated Med. Ins. Agents, L.L.C. v. G.E. Med. Protective Co.,* No. A03-1373, 2004 WL 615002, at *4 (Minn. Ct. App. Mar. 30, 2004).
17 *Equus*, 2002 WL 1634334, at *5 (citing *Int'l. Bus. Mach. Corp. v. Seagate Tech., Inc.*, 941 F. Supp. 98, 101 (D. Minn. 1992)).
18 *Lasermaster,* 931 F. Supp. at 637.
19 *Equus*, 2002 WL 1634334, at *4.
20 *Id.*
21 *Associated Med.*, 2004 WL 615002, at *4.

2. GENERAL KNOWLEDGE WITHIN A PARTICULAR INDUSTRY

Information that is not known to the general public, but widely known within an industry, is not a trade secret.[22] For instance, an executive's knowledge of contact people within a given industry is not a trade secret.[23]

3. GENERAL BUSINESS INFORMATION

General marketing intelligence or business plans do not constitute trade secrets.[24] Generally, courts will not protect broad categories of business information.[25]

4. VARIATIONS ON A WIDELY USED PROCESS

Variations on a widely used process do not constitute trade secrets.[26] Thus, a court refused to grant trade secret protection to a computer system that merely combined known subsystems.[27]

5. OBSOLETE INFORMATION

It should come as no surprise that obsolete information is not considered a trade secret, because the information has no economic value.[28] But the trick is defining when the information is considered obsolete. In one case, an executive's knowledge of telecast agreements that had been superseded by other agreements was not considered a trade secret, because his knowledge was obsolete.[29] Likewise, information regarding business strategies that was six months old was held obsolete, and therefore not a trade secret.[30]

6. EASILY REVERSE-ENGINEERED INFORMATION

If an item is available in the marketplace and easily reverse-engineered, then the item does not constitute a trade secret.[31]

7. PUBLICLY FILED INFORMATION

If information has been disclosed through a patent application, it no longer qualifies as a trade secret.[32] Likewise, other information that is submitted to a public body may lose trade secret protection. Thus, it is important to determine whether information that is submitted to a public body is protectable under an exception to state or federal open-records laws.

PRACTICAL PERSPECTIVE: One of the dilemmas a plaintiff seeks in any trade-secret action is that the litigation itself might result in disclosure of the trade secret. This risk is growing, because there is a trend towards requiring that a plaintiff plead the elements of its trade secret with a higher degree of specificity.[33]

22 *Fox Sports Net N., LLC v. Minn. Twins P'ship*, 319 F.3d 329, 336 (8th Cir. 2003).
23 *Id.*
24 *Newleaf Designs*, 168 F. Supp. 2d at 1044; *Seagate Tech.*, 941 F. Supp. at 100.
25 *Seagate Tech.*, 941 F. Supp. at 100.
26 *Electro-Craft*, 332 N.W.2d at 899.
27 *Id.* (citing *Jostens, Inc. v. Nat'l Computer Sys.*, 318 N.W.2d 691, 700-01 (Minn. 1982)).
28 *Fox Sports Net*, 319 F.3d at 336.
29 *Id.*
30 *Lexis-Nexis v. Beer*, 41 F. Supp. 2d 950, 959 (D. Minn. 1999).
31 *Electro-Craft*, 332 N.W.2d at 899.
32 *Coenco, Inc. v. Coenco Sales, Inc.*, 940 F.2d 1176, 1179 n.3 (8th Cir. 1991).
33 See Loftness Specialized Farm Equip. Inc. v. Twiestmeyer, Civ. No. 11-1506 (DWF/TNL), *2012 WL 1247232, at *7 (D. Minn. Apr. 13, 2012); Hot Stuff Foods, LLC v. Dornbach, 726 F. Supp. 2d 1038, 1044 (D. Minn. 2010); Luigino's Inc. v. Peterson, 317 F.3d 909, 912 (8th Cir. 2003); but see TE Connectivity Networks, Inc. v. All Sys. Broadband, Inc., Civ. No. 13-1356 ADM/FLN, 2013 WL 6827348, at *3 (D. Minn. Dec. 26, 2013) (holding that while a plaintiff may not rely on conclusory statements to establish its trade secrets, a plaintiff is not required to reveal exact parameters of a trade secret); Superior Edge, Inc. v. Monsanto Co., 964 F. Supp. 2d 1017, 1042 (D. Minn. 2013).*

III. WHAT RISK DOES YOUR COMPANY FACE?

Trade secret cases are distinguished from normal commercial disputes by the availability of a wider range of damages (including punitive damages), the possibility that the defendant will be responsible for the plaintiff's attorney fees, and the availability of injunctive relief.

A. DAMAGES: BIG TROUBLE

A plaintiff can recover both its lost profits and for any unjust enrichment the defendant received from the theft.[34] In lieu of damages measured by other means, a court may impose a reasonable royalty for the defendant's use of the trade secret.[35]

A trade secret defendant faces greater liability than the defendant in a normal commercial dispute. In a normal dispute, a defendant's maximum liability would be for the plaintiff's losses. A trade secret defendant is not only liable for the plaintiff's losses stemming from the misappropriation, but also for any unjust enrichment the defendant received from the misappropriation.[36] The only limitation is that the unjust enrichment damages cannot have been taken into account in determining the plaintiff's losses.[37]

For example, a hypothetical plaintiff in the business of manufacturing software has its development work stolen. As a result of the theft, defendant is able to put competing software on the market. Consequently, the plaintiff lost $10 million in sales, the defendant gained $10 million in sales, and the defendant saved $2 million in software development costs. In this scenario, the plaintiff could recover $12 million. It would be impermissible for the plaintiff to recover both its lost sales and the defendant's increased sales, because the defendant's increased sales have already been taken into account in calculating plaintiff's lost sales.

B. INJUNCTION MALFUNCTION

A defendant does not just face the possibility of a large damages award. The plaintiff is also entitled to enjoin the defendant from using the trade secret.[38] In our hypothetical scenario, the plaintiff would be entitled to an injunction preventing the defendant from selling the software.

The length of the injunction is determined by the period of time that would be required for independent development of the trade secret.[39] The time period of the injunction can be extended to eliminate any commercial advantage that a defendant derived from the misappropriation.[40]

The risk that a company faces is aptly illustrated by the Eighth Circuit's decision in the *Wyeth* case. The defendant was a pharmaceutical company that misappropriated another company's process for producing estrogen.[41] The Eighth Circuit upheld the district court's decision to permanently enjoin the defendant from producing estrogen.[42] The Eighth Circuit adopted the district court's reasoning that a permanent injunction was appropriate for two reasons: (1) no competitor had ever replicated the process during the decades the process had existed; and (2) the defendant had engaged in conduct, namely destroying evidence and giving false testimony, that demonstrated that the defendant could not be trusted to undertake future research into developing an alternative process without relying on the misappropriated trade secrets.[43] The injunction put the defendant out of business.

---

34 *Children's Broad. Corp. v. The Walt Disney Co.*, 357 F.3d 860, 865 (8th Cir. 2004) (citing Minn. Stat. § 325C.03(a)).
35 Minn. Stat. § 325C.03(a).
36 Minn. Stat. § 325C.03.
37 *Id.*
38 Minn. Stat. § 325C.02.
39 *Wyeth*, 2003 WL 22282371, at *27 (citing *Surgidev*, 648 F. Supp. at 696).
40 Minn. Stat. § 325C.02(a).
41 *Wyeth v. Natural Biologics, Inc.*, 395 F.3d 897, 899 (8th Cir. 2005).
42 *Id.* at 903.
43 *Id.*

PRACTICAL PERSPECTIVE: It may not always be in a company's best interest to immediately pursue an injunction if it only suspects theft. Rushing to seek injunctive relief without strong evidence of both a trade secret and misappropriation or inevitable misappropriation[44] of the trade secret risks an early adverse determination from a court that the company is unlikely to succeed on the merits. Once a court makes that determination, it will be difficult to reverse its initial impression and, at best, likely dooms a company to protracted litigation.

C. WILLFUL & MALICIOUS IS VICIOUS

In addition to lost profits, unjust enrichment, and reasonable royalties, a defendant can be liable for the plaintiff's attorneys' fees and for punitive damages up to twice the value of actual damages.[45] The defendant faces liability for the plaintiff's attorneys' fees and punitive damages if the misappropriation is willful and malicious.[46]

A trio of trade secret cases have identified the following conduct as willful and malicious:[47]

- Defendant's management is aware that it might be utilizing trade secrets, but proceeds with the project without investigating;
- Without informing the plaintiff of the defendant's decision to reject a business opportunity, defendant's management continues to solicit trade secrets under the pretext of negotiations and then transfers that information in violation of an express confidentiality agreement; and
- The defendant took information that it knew was confidential and used it to develop competing software.

PRACTICAL PERSPECTIVE: Nothing turns a problem into a catastrophe quicker than hiding, destroying, or altering evidence. Not only does this conduct constitute the independent tort of spoliation and risk serious sanctions, it makes juries, judges, and arbitrators mad, which leads to findings of willful and malicious misappropriation and big damages.

D. BAD FAITH

Attorneys' fees may also be awarded if a claim of misappropriation is made in bad faith, or a motion to terminate an injunction is made or resisted in bad faith.[48] A party may be liable under this theory if it can be shown that there is a complete lack of evidence supporting the claim and the party had subjective misconduct in bringing or maintaining the claim.[49] However, courts have held that a trade secret claim is not brought in bad-faith if it survives summary judgment[50] or does not merit sanctions.[51] If you suspect that there may be the potential for an award of fees for malicious/willful misappropriation or bad faith in bringing the claim, counsel should take care to differentiate the fees incurred in furtherance of the trade secret claim, verses other claims in the lawsuit.

---

44 To establish inevitable misappropriation, the party seeking the injunction has the heavy burden of establishing a "high degree of probability" that the party possessing the trade secret will inevitably disclose it. Honeywell Int'l Inc. v. Stacey, No. 13-CV-3056 (PJS/JJK), 2013 WL 9851104, at **6 (D. Minn. Dec. 11, 2013).*

45 Minn. Stat. §§ 325C.04, 325C.03(b).

46 *Id.*

47 *Scott Equip. Co.*, 2003 WL 21804868, at *3 (management knowledge); *K-Sun Corp.*, 1998 WL 422182, at *4 (continued solicitation and violation of express agreement); *Zawels v. Edutronics, Inc.*, 520 N.W.2d 520, 524 (Minn. Ct. App. 1994) (knowing use to develop software).

48 Minn. Stat. § 325C.04.

49 *Norwood Operating Co. v. Beacon Promotions, Inc.*, Civ. No. 04-1390 (MJD/SRN), 2006 WL 3103154, at *1-2 (D. Minn. Oct. 31, 2006).

50 *Id.* at *3; *Wixon Jewelers, Inc. v. Aurora Jewelry Designs*, No. C0-01-2149, 2002 WL 1327014, at * 2 (Minn. Ct. App. June 18, 2002).

51 *Weaver v. Iverson*, No. A12-0354, 2012 WL 3641358, at *2 (Minn. Ct. App. Aug. 27, 2012).

IV. WHEN DO TRADE SECRET CLAIMS ARISE?

A party's potential trade secret liability is determined in part by the relief the plaintiff is seeking. In order for a trade secret plaintiff to prevail on an injunction, the plaintiff must show the threat of misappropriation or actual misappropriation.[52] The threat of misappropriation is established if the party seeking the injunction can show there is "a high degree of probability of inevitable disclosure."[53] A party can establish actual misappropriation either by direct or circumstantial evidence.[54]

Although almost any business relationship can give rise to trade secret liability, several scenarios pose an especially high risk. The following examples are based on the scenarios most frequently presented by Minnesota case law.

A. EMPLOYMENT RELATIONSHIPS

Any new hire has the potential for bringing misappropriated trade secrets with her. Moreover, even if your company has not used the information, it might still be subject to an injunction under the inevitable disclosure doctrine.[55]

B. BUSINESS ACQUISITIONS/EQUITY FUNDING

Trade secret claims commonly arise in the context of business acquisitions. The *K-Sun* case illustrates the dangers that a company can face in the context of an acquisition. Unsuccessful merger negotiations in *K-Sun* led to the defendant company being liable for attorneys' fees and punitive damages.[56] Other Minnesota cases illustrate that the bad feelings that often arise from a failed acquisition can give rise to trade secret claims.[57]

A business that is trying to raise capital also faces trade secret challenges. Despite the disclosure requirements imposed by securities law, a company must take steps to guard its trade secrets during the fundraising process. At a minimum, the capital-raising company should have non-disclosures in place with potential investors. Otherwise, the company faces the possibility that the potential investors will become competitors. Needless to say, this scenario presents a high litigation risk.

C. MANUFACTURING/MARKETING CONTRACTS

Contracts to manufacture complex goods that involve the exchange of technical information between the seller and buyer can give rise to trade secret claims. Likewise, trade secret liability can arise when one company offers another company the opportunity to market its product. If the other company refuses and then starts to market a similar product, that company faces a substantial litigation risk.

V. HOW TO PROTECT YOUR COMPANY AGAINST A TRADE SECRET CLAIM

A. EMPLOYEE SCREENING

Any new hire should be screened to see if that hire has any knowledge regarding her former employer's trade secrets. The level of screening should increase if the employee is going to be involved in your company's core business operations or research and development. The screening should focus on the employee's actual technical knowledge as opposed to general knowledge or skills that the employee gained at his previous job.[58]

52 Minn. Stat. § 325C.02.
53 *Lexis-Nexis,* 41 F. Supp. 2d at 958 (citations omitted).
54 *Wyeth,* 2003 WL 22282371, at *21 (citing *Pioneer Hi-Bred Int'l v. Holden Found. Seeds, Inc.,* 35 F.3d 1226, 1239 (8th Cir. 1994)).
55 *Lexis-Nexis,* 41 F. Supp. 2d at 959.
56 *K-Sun*, 1998 WL 422182, at *1-4.
57 *See*, *e.g.*, *Luigino's,* 2002 WL 122389.
58 *Lasermaster,* 931 F. Supp. at 636-37 ("The concept of a trade secret does not include a man's aptitude, his skill, his dexterity, his manual and mental ability, and such other subjective knowledge as he obtains while in the course of his employment ... the right to use and expand these powers remains his property. ...") (citation, internal quotation marks and alterations omitted).

New employees should be instructed not to disclose or use a former employer's trade secret information in connection with their employment with your company. Additionally, new employees should be required to attest to the following in an offer letter or employment agreement:

"If Employee possesses any information that s/he knows or should know is considered by any third party, such as a former employer of Employee's, to be confidential, trade secret, or otherwise proprietary, Employee shall not disclose such information to Company or use such information to benefit Company in any way."

Similarly, new employees should attest to the following in an offer letter or employment agreement:

"Employee represents and warrants to Company that s/he is not under, or bound to be under in the future, any obligation to any person, entity, firm, or corporation that is or would be inconsistent or in conflict with, or would prevent, limit, or impair in any way Employee's employment by the Company."

Supervisors should monitor their supervisees to ensure that they are not using a former employer's trade secrets in connection with their work for your company. If such conduct is occurring, the company should take prompt action to put a stop to such conduct (including disciplinary action against the offending employee) and cease any and all use of the trade secret information.

B. PERMISSION

Permission is the simplest way to avoid a trade secret claim. Generally, no misappropriation occurs where the defendant has received the plaintiff's express or implied consent to disclose the secret.[59] Moreover, requesting permission defeats the notion that the use was willful and malicious, unless the defendant is denied permission and proceeds anyway.

C. CLEAR DEFINITIONS

When your company enters into funding, acquisition, or marketing discussions, it should have an agreement in place that identifies precisely what information is being exchanged and who has access to the information. Conversely, the agreement should define what information is not covered. Finally, the agreement should provide for return of the information and reasonable restrictions on the information's use.

D. HONESTY IS THE BEST POLICY

Often trade secret claims arise out of the frustration of a failed business relationship. That frustration is compounded if one party feels that it was led along so it could be mined for information. It is important to manage expectations during negotiations and clearly inform the other business when negotiations have reached an impasse.

VI. HOW TO PROTECT YOUR COMPANY'S TRADE SECRETS

A trade secret owner must take reasonable measures to protect secrecy.[60] This reasonableness test is based on the particular circumstances of both the secret itself and the business.[61] The touchstone test for determining whether a company's security measures are adequate revolves around notice: "[i]f, under all the circumstances, the employee knows or has reason to know that the owner intends or expects the information to be secret, confidentiality measures are sufficient."[62]

Circumstances which may be reasonable at one time and under one set of circumstances may cease to be reasonable at another time or under other circumstances. Accordingly, it is appropriate for an enterprise to modify, typically by enhancing, its security procedures in order to respond to new challenges. The modifications are not evidence that prior procedures were inadequate, but rather are a legitimate exercise in imposing reasonable secrecy safeguards.

59 Minn. Stat. § 325C.01, subd. 3.
60 Minn. Stat. § 325C.01, subd. 5.
61 *Id.*
62 *Lasermaster,* 931 F. Supp. at 635.

Techniques that can be employed to protect a secret are numerous. As a practical matter the care exercised tends to correspond to the economic value of the secret and its nature; some secrets are more readily protected with minimal effort than others can be with even extensive care. This means that a company's failure to employ the fullest range of protective techniques will not terminate the secrecy, provided that they were, in and of themselves, reasonably prudent.

A. EVERYTHING MEANS NOTHING

As discussed throughout the rest of this section, there are a number of policies that a company can adopt to protect its trade secrets. But the adoption of the policies is not enough. A company must consistently follow its policies to make sure that it has not waived trade secret status on any particular information.[63] Remember that the defense in a trade secret case will focus on your company's lapses.

Because these policies' expenses are related to the volume of information that a company is trying to manage, many companies would be better served if they identified their core trade secrets and only attempted to protect them. Moreover, because a larger volume of information creates a stronger potential for lapses, managing less information will probably make that core information more secure. Finally, if everything is defined as a trade secret, a company dilutes the notice it is providing on the information it is most interested in protecting. This potentially weakens a company's trade-secret claim.[64]

B. STAMPING OUT THEFT

Courts routinely consider whether documents used both in-house and those circulated to third parties are marked or stamped as "confidential" or "secret."[65] Moreover, a business must make sure that it follows its own procedures, or risk losing trade secret status. In one case, a business required that any trade secrets be stamped confidential, but failed to stamp the information it sought to protect.[66] The court found that the business's failure to stamp the documents indicated that it had failed to take reasonable measures to protect them.[67]

Additionally, a business should have a policy in place for dealing with waste documents. Discarded plans or drawing should be shredded, not just thrown away.[68]

C. NON-DISCLOSURE: AN OUNCE OF PREVENTION

Employers seeking to provide their confidential and trade secret information are well-advised to enter into non-disclosure agreements with their employees. Employers should give special attention to how "confidential information" is defined in the agreement to ensure that the definition captures all of the company's secret information, including the information that is uniquely secret to the company. One benefit of a non-disclosure agreement is that it can protect a broader category of information than just trade secrets. Confidential information that does not qualify as a trade secret still qualifies for protection under a non-disclosure agreement.[69] Additionally, non-disclosure agreements should require employees not to disclose the company's confidential information during their employment and *for all time* following the end of their employment. Employers are encouraged to consult legal counsel in connection with drafting and implementing non-disclosure agreements.

Although a non-disclosure agreement is an important tool for protecting trade secrets, it, alone, is not enough.[70] A company's security measures will be deemed reasonable only if it follows the procedures outlined in the non-disclosure agreement and takes other steps to secure its trade secrets, including

63 *Lexis-Nexis,* 41 F. Supp. 2d at 959.
64 *See*, *e.g.*, *Menzies Aviation (USA), Inc. v. Wilcox*, 978 F. Supp. 2d 983, 995 (D. Minn. 2013).
65 *Avidair Helicopter Supply, Inc.*, 663 F.3d at 974 (citing *Wyeth*, 395 F.3d at 899-900 & n.4).
66 *Lexis-Nexis*, 41 F. Supp. 2d at 959.
67 *Id.*
68 *Electro-Craft,* 332 N.W.2d at 902.
69 *Relco, LLC v. Keller*, No. A13-1633, 2014 WL 2921895, at *6 (Minn. Ct. App. June 30, 2014) (citing *Cherne Indus., Inc. v. Grounds & Assocs., Inc.*, 278 N.W.2d 81, 90 (Minn. 1979)).
70 *Coyne's & Co., Inc. v. Enesco, LLC*, Civ. No. 07-4095 (MJD/SRN), 2010 WL 3269977, at *16 (D. Minn. Aug. 16, 2010); *Storage Tech. Corp. v. Cisco Sys., Inc.*, Civ. No. 00-2253 (JNE/JGL), 2003 WL 22231544, at *7 (D. Minn. Sept. 25, 2003) (citing *Electro-Craft,* 332 N.W.2d at 902).

pursuing claims against employees who violate their non-disclosure obligations.[71] Moreover, where a company has a non-disclosure agreement, those contractual duties will define whether a misappropriation has taken place.[72] Thus, a company will want to carefully define what constitutes a permissible use; otherwise, a loose definition can effectively grant the other party permission to use a company's trade secrets.

D. NON-COMPETITION AGREEMENTS

Most states, including Minnesota, will enforce reasonable employee non-competition agreements. Non-competition agreements prohibit a former employee from working for a competitor in the company's trade area for a reasonable period of time following employment. Non-competition agreements may also prohibit a former employee from soliciting the company's customers and/or employees for a reasonable period of time following employment. While there is no bright-line rule with regard to the permissible duration of such agreements, most courts have held that post-employment restrictions lasting one year are reasonable. Non-competition agreements must be drafted as narrowly as possible so as to not unduly restrict the employee's ability to earn a livelihood. While Minnesota courts have the discretion to modify an overbroad agreement so as to make it reasonable, some states do not allow judicial modification and instead invalidate an overbroad agreement in its entirety.

Non-competition agreements must be supported by consideration. That is, the employee must be given something of value to which he or she is not otherwise entitled in exchange for his or her agreement to be bound by a non-competition agreement. In Minnesota, for new employees, the new employment itself is adequate consideration provided the employee was notified of the requirement and signed the non-competition agreement prior to commencing employment. If an existing employee is asked to sign a non-competition agreement under Minnesota law, the employer must give the employee something more than mere continued employment as consideration for the agreement. For example, the employer may elect to give the employee a pay raise, signing bonus, stock options, a new bonus plan or the like, provided the employee was not already entitled to such benefit in the normal course of employment.

There are two employment law trends that have weakened the enforceability of non-compete agreements. First, some major states have either refused to enforce non-competition agreements (e.g. California)[73] or have placed substantial limitations on their enforceability. For example, Illinois state courts have held that there must be at least two years or more of continued employment to constitute adequate consideration to enforce a restrictive covenant.[74] While one federal court has adopted this approach,[75] three federal judges in Illinois have rejected this line of reasoning, predicting that the Illinois Supreme Court would not adopt such a bright-line rule.[76] Second, there is at least one significant decision refusing to enforce a choice-of-law provision that would have avoided a jurisdiction's law that refused to enforce a non-compete agreement.[77]

Because non-competition agreements call into question additional drafting and enforceability issues, employers are encouraged to consult legal counsel in connection with such agreements.

---

71 *See id.*

72 *Coyne's & Co.*, 2010 WL 3269977, at *16.

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

74 *See, e.g., Fifield v. Premier Dealer Servs., Inc.*, 993 N.E.2d 938, 943 (Ill. App. Ct. 2013) (collecting cases).

75 *Instant Tech., LLC v. DeFazio*, No. 12 C 491, 2014 WL 1759184, at *14 (N.D. Ill. May 2, 2014) ("This court, however, predicts the Illinois Supreme Court upon addressing the issue would not alter the doctrine established by the recent Illinois appellate opinions, which clearly define a 'substantial period' as two years or more of continued employment.").

76 *Cumulus Radio Corp. v. Olson*, No. 15-CV-1067, 2015 WL 643345, at *4 (C.D. Ill. Feb. 13, 2015) ("[T]the Court does not believe that the Illinois Supreme Court would adopt the bright-line test announced in *Fifield*."); *Bankers Life & Cas. Co. v. Miller*, No. 14 CV 3165, 2015 WL 515965, at *4 (N.D. Ill. Feb. 6, 2015) ("The Illinois Supreme Court would . . . reject a rigid approach to determining whether a restrictive covenant was supported by adequate consideration; it would not adopt a bright-line rule requiring continued employment for at least two years in all cases."); *Montel Aetnastak, Inc. v. Miessen*, 998 F. Supp. 2d 694, 716 (N.D. Ill. 2014) ("Given the contradictory holdings of the lower Illinois courts and the lack of a clear direction from the Illinois Supreme Court, this Court does not find it appropriate to apply a bright line rule.").

77 *Ascension Ins. Holdings, LLC v. Underwood*, C.A. No. CV 9897-VCG, 2015 WL 356002 (Del. Ch. Jan. 28, 2015) (holding that a Delaware choice of law and venue provision in an employment agreement, which purported to impose non-competition requirements, was not controlling because California law would otherwise apply to the agreement and California's interest in preventing the enforcement of a covenant not to compete—against a California resident, employed in California, and seeking to compete largely in California—was greater than Delaware's interest in freedom of contract).

E. PHYSICAL SECURITY

Secret use protects an existing trade secret. In contrast, a purportedly secret process which is employed in a plant with little or no measures to keep it from public view ceases to be a secret. A Minnesota court held that reasonable measures did not exist where the plaintiff had twice held an open house where the public was invited to observe the manufacturing process.[78]

Companies must take reasonable precautions to protect secret information from discovery by those outside the company, including implementing measures to physically protect the secret information. For example, a company's practice of keeping trade secret documents in locked rooms or files is frequently cited as a reasonable precaution.[79] Failure to keep sensitive drawings or documents in a central and locked location will often defeat a trade secret claim.[80]

Similarly, restricting visitors to sensitive areas of a plant or facility will protect trade secrets.[81] Additional security measures can include the following: requiring employee ID badges, requiring that visitors sign in with proper identification and questioning and removing unknown persons from the property.[82] Failure to restrict visitor access can defeat a trade secret claim.[83]

Securing entrances to buildings and certain sensitive areas within facilities is also important. Where a plant had a few guarded entrances, but unlocked doors existed without warning signs limiting access, the Minnesota Supreme Court found that the owner had not taken reasonable measures.[84] Physical security measures prevent third party access and are also a way of signaling to employees that certain information is secret.[85]

F. PUBLICATION POLICIES

The policies may include a screening process for all outgoing publications and speeches to ensure that no confidential information is disseminated.[86] A trade secret may be lost through disclosure occurring in advertising, trade circulars, or in an analogous manner. For example, if the owner of proprietary data permits it to be published for government procurement purposes, absent express contractual or statutory protection, trade secret protection will be lost. Additionally, if a company publishes what it later claims to be confidential information on its website (e.g., customer names, pricing), the company will lose protection with regard to another's use of such information. Adherence to a screening process for all publications can prevent inadvertent disclosure.

PRACTICAL PERSPECTIVE: Pride goeth before the fall. Two relatively innocuous events—plant tours and seminar presentations—can place a company's trade secrets in danger. Although it is easy to understand a company taking pride in its accomplishments, you must be careful not to disclose your trade secrets through these events. A company should segregate any sensitive processes or technology from a plant tour and carefully monitor employee presentations.

G. DIVISION OF INFORMATION

Internal secrecy can be maintained by dividing a manufacturing or development process into steps or separating the various departments working on the several steps. Courts have found that separating sensitive departments or processes from the central facility or plant is a reasonable step in protecting secrets.[87]

78 *Electro-Craft*, 332 N.W.2d at 903.
79 *Surgidev*, 648 F. Supp. at 693-94 (citations omitted).
80 *Electro-Craft*, 332 N.W.2d at 902.
81 *Surgidev*, 648 F. Supp. at 693.
82 *Id.*; *Electro-Craft*, 332 N.W.2d at 902.
83 *Surgidev*, 648 F. Supp. at 693.
84 *Electro-Craft*, 332 N.W.2d at 902
85 *Id.*
86 *Id.* at 901-02.
87 *Surgidev*, 648 F. Supp. at 693.

H. NEED TO KNOW

A trade secret does not lose its character by being confidentially disclosed to employees, without whose assistance it would be valueless. But a trade secret owner must be scrupulous in confidentiality strictures with its employees and disseminate trade secrets only to employees on a "need-to-know" basis—for example, providing field representatives with sales information for their assigned territory only and managers with information for those they supervise only.[88]

Employees having such access should be carefully cautioned as to the trade secret status of matters on which they work. Some companies require that employees meet with the legal department to discuss secrecy at the start of their employment.

I. COMPUTER SECURITY MEASURES

Sensitive information is often stored on computers. Companies should limit access to computers and systems through passwords and keep magnetic tapes, flow charts, symbolics and source codes under lock and key when not in use. Policies regarding employee use and travel with laptop computers containing trade secret information should also be in place. There may also be independent remedies under federal statute, discussed in further detail below.

VII. CLAIMS UNDER THE COMPUTER FRAUD & ABUSE ACT

Beyond trade secret law, another popular avenue to protect companies' confidential information is a federal civil cause of action under the Computer Fraud and Abuse Act for unauthorized access to information. The Computer Fraud & Abuse Act ("CFAA"), 18 U.S.C. § 1030, is a federal statute that makes it unlawful for persons to engage in several forms of computer fraud and abuse, including:

- Accessing, without authorization, certain computer systems;
- Exceeding the scope of authorization; and
- Causing damage to computer systems or data maintained on those systems.

Employees who misappropriate trade secrets using computers may be in violation of the CFAA.
The CFAA does not require proof of the elements of a trade secret. In contrast to trade secrets law, the CFAA only requires an employer to prove that the employee accessed the computer "without authorization" or that the employee exceeded authorized access. "[E]xceeds authorized access" is defined as accessing "a computer with authorization and [using] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[89]

However, "without authorization" is not defined by the statute. A decision from the Fourth Circuit highlights the split between the federal circuits over the scope of the CFAA and whether it extends to employees who steal an employer's trade secrets to which they were lawfully given access as employees.[90] WEC gave its employee a company laptop and granted him access to the company's servers and intranet that contained "numerous confidential and trade secret documents," including pricing terms, information on pending projects, and other technical information. WEC had written policies prohibiting employees from (1) using any company information without authorization or (2) downloading it to a personal computer. However, the policies did not restrict the employee's authorization to access the information. The employee resigned and joined a direct competitor, but while still employed by WEC, downloaded a number of confidential documents from the company's servers and emailed them to his personal email account. He and his assistant also downloaded confidential information to a personal computer.

The district court dismissed the CFAA claim and found that WEC's computer policies only limited the "use of information not access to that information."[91] The court concluded that no liability was warranted under the CFAA because the employee was allowed to access the information at issue as an employee. The Fourth Circuit

88 *Id.* at 694.
89 18 U.S.C. § 1030(e)(6).
90 *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012).
91 *Id.* at 202.

Court of Appeals affirmed the district court's interpretation of the CFAA, suggesting that reading the CFAA too broadly could result in potential liability for any employee who "checked the latest Facebook posting or sporting event scores in contravention of his employer's use policy."[92]

Not surprisingly, there is a split among the federal circuits regarding what constitutes unauthorized access under the CFAA. Under the narrow view adopted by the Fourth and Ninth Circuits, an employee granted access to a computer in connection with his employment is "authorized" to access that computer under the CFAA regardless of his or her intent or whether internal policies limit the employee's use of the information accessed.[93] A majority of circuit courts have taken a broader view of "without authorization," concluding that an employee who is granted access to a computer in connection with his or her employment may exceed his or her authority by misusing the information on the computer, either by severing the agency relationship through disloyal activity, or by violating employer policies and/or confidentiality agreements.[94]

It is important to note, however, that damages under CFAA may be limited to actual computer impairment; recovery of consequential damages or damages for other injuries associated with the misappropriation of confidential information may not be typically authorized.[95]

CONCLUSION

Failing to manage trade-secret information puts the very existence of a company at risk. A company can lose its investment in research and development, see its margins erode, and face large verdicts that include punitive damages and attorneys' fees. In the worst case, a court could issue an injunction that shuts down a critical product. Given the risks associated with mismanaging trade-secret information, a minimal upfront investment in establishing policies and procedures can prevent catastrophic damage to a business. Every company should have policies in place for managing trade-secret information.

Jeffrey Post is the primary author of this article. Jeffrey is a shareholder at the law firm of Fredrikson & Byron, P.A. in Minneapolis, Minnesota. His practice includes both trade-secret litigation and counseling to avoid litigation.

Ingrid Culp, Timothy O'Shea, and Anupama Sreekanth also contributed to this article.

Ingrid is also a shareholder at Fredrikson & Byron, and her practice focuses on employment law counseling.

Timothy is a shareholder at Fredrikson & Byron, P.A., whose practice focuses on intellectual property litigation.

Anupama Sreekanth is an associate at Fredrikson & Byron, P.A., who practices in the area of commercial litigation.

More detailed biographies are available for all the attorneys at fredlaw.com.

92 *Id.* at 206.

93 *See id.* at 205-06; *United States v. Nosal*, 676 F.3d 854, 857-59 (9th Cir. 2012) (en banc); *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1132-35 (9th Cir. 2009)).

94 *United States v. John*, 597 F.3d 263, 271-73 (5th Cir. 2010); *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010); *Int'l Airport Ctrs. LLC v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006); *Ef Cultural Travel Bv v. Explorica, Inc.*, 274 F.3d 577, 582 (1st Cir. 2001)); *see also Reliable Prop. Servs., LLC v. Capital Growth Partners, LLC*, 1 F. Supp. 3d 961, 964 (D. Minn. 2014) ("When George used his access not to help maintain the SnowMaster software, but instead to analyze and compile customer data to further his own interests, George almost certainly 'exceed[ed] authorized access' for purposes of § 1030(a)(2).").

95 *Harley Auto. Grp.*, 2013 WL 6801221, at *6 (collecting cases).