

SOUTHERN LAW JOURNAL

OFFICIAL PUBLICATION OF THE SOUTHERN ACADEMY OF LEGAL STUDIES IN BUSINESS

WWW.SALSB.ORG

VOLUME XXXI

FALL 2022

NUMBER 1

ARTICLES:

APPROPRIATION OF LIKENESS AND INFORMED CONSENT IN THE
AGE OF SURVEILLANCE CAPITALISM

(PP. **-**)

**Roger W. Reinsch
Sonia Goltz
Marat Bakpayev**

THE BATTLE OVER FIDUCIARY RESPONSIBILITY OF PENSION FUND
MANAGERS: THE TRUMP ADMINISTRATION TAKES ON THE ESG
MOVEMENT

(PP. **-**)

**Frank J. Cavaliere
Ricardo Colon
Toni Mulvaney
Marleen Swerdlow**

PRACTICAL STRATEGIES TO PROTECT CORPORATE TRADE SECRETS
AND AVOID MISAPPROPRIATION CLAIMS

(PP. **-**)

**Wade Davis
Jeffrey Post**

SEXUAL HARASSMENT CLAIMS IN FEDERAL COURT:
AN EMPIRICAL ANALYSIS

(PP. **-**)

Alix Valenti

THE NEED FOR COMPREHENSIVE FEDERAL LEGISLATION
TO REGULATE FACIAL RECOGNITION TECHNOLOGY

(PP. **-**)

Winston Spencer Waters

STRIVING FOR PIZZA FOR EVERYONE OR JUST MORE CALIFORNIA
VAMPIRES?

(PP. **-**)

Christopher L. Thompson

BEARING THE COSTS ASSOCIATED WITH SEX TRAFFICKING

(PP. **-**)

**Christina A. Culver
Benjamin Ritz
Diana Brown**

PEDAGOGY:

HAUNTINGLY FUN LEGAL ENVIRONMENT OF BUSINESS TOPICS
FOR A HALLOWEEN-THEMED CLASS

(PP. **-**)

Michael Conklin

EXPLORING THE ETHICAL AND INSTRUCTIONAL POSSIBILITIES OF
GROUPME IN BUSINESS LAW AND BUSINESS COMMUNICATION
COURSES

(PP. **-**)

**Lindsay Clark
Ashton Mouton
Traci Austin**

PRACTICAL STRATEGIES TO PROTECT CORPORATE TRADE SECRETS AND AVOID MISAPPROPRIATION CLAIMS

WADE DAVIS*
JEFFREY POST**

I. INTRODUCTION

As one of the four principle categories of intellectual property rights, along with patents, copyrights, and trademarks, knowledge of trade-secret law is essential to conducting business and thriving in today's economy. The U.S. Chamber of Commerce estimates that trade secrets protect U.S. assets worth an estimated 5 trillion and 5.5 trillion dollars.¹⁹⁷ Many businesses view trade secret protection as more critical than any other form of intellectual property - including patents.¹⁹⁸

Knowledge of trade secrets might be the difference between protecting critical business assets or them ending up in a competitor's hands. It may also mean the difference between facing a large jury verdict and reaching a quick, favorable resolution to a claim. By focusing on the Federal Defend Trade Secrets Act and Minnesota's application of the Uniform Trade Secret Act, this article provides a practical guide to understand how these statutes operate in a real business environment. As always, businesses should seek legal advice regarding the details of the Act's implementation in their particular jurisdiction. This article does not provide legal advice; rather, it is designed to help companies and legal practitioners spot red flags in their operations and strategically protect their trade secrets and intellectual property.

This article provides a practical overview to trade secret law for businesses seeking to protect their trade secrets and avoid trade secret claims. Section I identifies the types of information that are protectable as a trade secret and common categories that are often not protectable. Section II discusses ways that trade secrets can be misappropriated and common defenses to misappropriation. Section III examines the damages

* J.D., Associate Professor of Business Law, Minnesota State University, Mankato.

** Shareholder at Fredrikson and Byron, P.A.; J.D, University of Minnesota.

¹⁹⁷ Brian T. Yeh, *Protection of Trade Secrets: Overview of Current Law and Legislation*, Congressional Research Service, at 13, Apr. 22, 2016; U.S. Chamber of Commerce, *The Case for Enhanced Protection of Trade Secrets in the Trans-Pacific Partnership Agreement*, at 10, available at https://www.uschamber.com/sites/default/files/legacy/international/files/Final%20TPP%20Trade%20Secrets%208_0.pdf

¹⁹⁸ *Id.*

and remedies that are available. Section IV describes proactive steps companies can take to head-off trade secrets claims asserted by others. Section V offers recommendations to protect a company's trade secrets from misappropriation by others. Finally, Section VII identifies common companion claims brought in trade secret litigation.

II. DEFINING TRADE SECRETS

A wide variety of information potentially qualifies as a trade secret, including “all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes.”¹⁹⁹ Trade secrets are protected under common law, state statutes, and the Federal Defend Trade Secrets Act.²⁰⁰ As explained in this section, information must meet an additional three-factor test before it can be considered a trade secret.²⁰¹

With the exception of New York, every state in has adopted the Uniform Trade Secrets Act in one form or another.²⁰² New York relies on common law, including Section 757 of the Restatement of torts, and criminal law to govern trade secrets protection and claims.²⁰³ Although the federal statute does not preempt or displace any other trade secrets claims or remedies, the state uniform trade secrets statutes often “displace conflicting tort, restitutionary, and other law of this state providing civil

¹⁹⁹ 18 U.S.C. § 1839(3); MINN. STAT. § 325C.01; Berkley Risk Adm'rs Co., LLC v. Accident Fund Holdings, Inc., Civ. No. 16-2671, 2016 U.S. Dist. LEXIS 113421, (D. Minn. Aug. 24, 2016) (“The definition of ‘trade secret’ in the federal statute and MUTSA are substantially similar.”).

²⁰⁰ See *cf.*, 18 U.S.C. §1831 et seq. (federal “Defend Trade Secrets Act”), MINN. STAT. Ch. 325C (Minnesota “Uniform Trade Secrets Act). Parties can use the Defend Trade Secrets Act to establish jurisdiction in federal court. CH Bus Sales, Inc. v. Geiger, No. 18-cv-2444; 2019 WL 23374492019 U.S. Dist. LEXIS 92067, *4 (D. Minn. Jun. 3, 2019) (remanding lawsuit back to state court where dismissed federal trade secret claim was the only basis for federal jurisdiction).

²⁰¹ 18 U.S.C. § 1839(3); MINN. STAT. § 325C.01; Electro-Craft Corp. v. Controlled Motion, Inc., 332 N.W.2d 890, 899-902 (Minn. 1983).

²⁰² See Peter Steinmeyer, *Massachusetts Becomes 49th State to Adopt Uniform Trade Secrets Act*, EPSTEIN BECKER GREEN (Aug. 21, 2018) (noting that more recently Massachusetts became the 49th state to adopt the UTSA). The Uniform Trade Secrets Act, published by the Uniform Law Commission in 1979 and amended in 1985, is a uniform law proposed for adoption by individual states.

²⁰³ See, e.g., Paz Sys., Inc. v. Dakota Grp. Corp., 514 F. Supp. 2d 402, 407 (E.D.N.Y. 2007); E.J. Brooks Co. v. Cambridge Sec. Seals, 105 N.E.3d 301, 316 (N.Y. 2018).

remedies for misappropriation of trade secrets²⁰⁴” but does not affect contract and civil remedies not based on trade secrets, or criminal remedies.

A. Information - Trade Secret Requirements

First, the information must not be generally known or readily ascertainable to be protected.²⁰⁵ If the information is “available in trade journals, reference books, or published materials,” the information is generally known.²⁰⁶ 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.²⁰⁷ 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.”²⁰⁸ 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.²⁰⁹ For instance, a compilation of publicly available information may constitute a trade secret if significant effort was necessary to compile the information, the information is not readily ascertainable, and it affords a competitive advantage.²¹⁰

Second, the information must gain independent economic value from not being generally known.²¹¹ “Generally, if substantial time and money would be required of a competitor to develop the same information,

²⁰⁴ MINN. STAT. §325C.07.

²⁰⁵ *Id.*; *Electro-Craft Corp.*, 332 N.W.2d at 897 (“Without a proven trade secret there can be no action for misappropriation, even if defendants’ actions were wrongful.”).

²⁰⁶ *Surgidev Corp. v. Eye Tech., Inc.*, 648 F. Supp. 661, 688 (D. Minn. 1986).

²⁰⁷ *Scott Equip. Co. v. Stedman Mach. Co.*, Civ. No. 06-906, 2003 WL 21804868, *2 (D. Minn. July 31, 2003).

²⁰⁸ *Surgidev*, 648 F. Supp. at 688 (citing *Electro-Craft*, 332 N.W.2d 890).

²⁰⁹ *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, 2011 WL 1885465, *8 (D. Minn. May 18, 2011).

²¹⁰ *AvidAir*, 663 F.3d at 972; *but see Strategic Directions Group v. Bristol-Myers Squibb Co.*, 293 F.3d 1062, 1065 (8th Cir. 2002) (compilation of known information is insufficient to establish trade secret); *Berkley Risk Adm’rs Co.*, 2016 U.S. Dist. LEXIS 113421 at *5-6.

²¹¹ 18 U.S.C. § 1839(3)(B); *Electro-Craft*, 332 N.W.2d at 900.

that information has economic value.”²¹² 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.²¹³

Third, a plaintiff must show that it made reasonable efforts to maintain the secrecy of the trade secret.²¹⁴ Trade secret law “does not require the maintenance of absolute secrecy; only partial secrecy or qualified secrecy has been required under the common law.”²¹⁵ 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.”²¹⁶ The law is also clear that the mere existence of a confidentiality agreement is insufficient to establish that the covered information constitutes a trade secret.²¹⁷

PRACTICE POINTER: Evaluating whether information constitutes a trade secret is difficult and experienced counsel is a necessity. Often, the more technical the information a company is seeking to protect, the more likely a jury, judge, or arbitrator is to consider the information is a trade secret. Thus, the process for coating a medical device will more likely be treated as a trade

²¹² *Surgidev*, 648 F. Supp. at 692; see also *AvidAir*, 663 F.3d at 973 (holding that the key question is not whether duplication is possible, but “whether the duplication of the information would require a substantial investment of time, effort, and energy.”).

²¹³ *Wyeth v. Natural Biologics, Inc.*, Civ. No. 98-2469, 2003 WL 22282371, *19 (D. Minn. Oct. 2, 2003); *I-Sys., Inc. v. Softwares, Inc.*, Civ. No. 02-1951, 2004 WL 742082, *14 (D. Minn. Mar. 29, 2004).

²¹⁴ 18 U.S.C. § 1839(3)(A); *Electro-Craft*, 332 N.W.2d at 901.

²¹⁵ *Surgidev*, 648 F. Supp. at 692-93.

²¹⁶ *K-Sun Corp. v. Heller Invs., Inc.*, Nos. C4-97-2052, C6-97-2053, 1998 WL 422182, *3 (Minn. Ct. App. July 28, 1998); *Macy’s Retail Holdings, Inc. v. Cty. of Hennepin*, 27-CV-13-6683, 2018 Minn. Tax LEXIS 16, *11-12 (Minn. Tax. Ct. Mar. 12, 2018) (maintaining confidentiality agreements with lenders, accountants, auditors, and prospective buyers” constitutes reasonable efforts to maintain secrecy).

²¹⁷ *Electro-Craft*, 332 N.W.2d at 901-02; *Bison Advisors LLC v. Kessler*, Civ. No. 14-3121, 2016 U.S. Dist. LEXIS 107244, 2016 WL 4361517, *11 (D. Minn. Aug. 12, 2016) (granting summary judgment to dismiss trade secrets claim where defendants signed confidentiality agreement because they did not otherwise treat information as confidential); *Coyne’s & Co. v. Enesco, LLC*, No. 07-4095, 2010 U.S. Dist. LEXIS 83630, 2010 WL 3269977, *16 (D. Minn. Aug. 16, 2010); *RING Comput. Sys., Inc. v. ParaData Comput. Networks, Inc.*, No. C4-90-889, 1990 Minn. App. LEXIS 922, 1990 WL 132615, *2 (Minn. Ct. App. Sept. 10, 1990) (holding that “signing of a confidentiality agreement, without more, is not enough”).

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 will be protected. Finally, a trade secret must be describable in a fashion that a judge or jury can understand. When evaluating a client's trade-secret claim, we often utilize the one-sentence test. Parties who can explain their trade secret in one sentence generally have a stronger claim than those who cannot.

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 a trade secret. Furthermore, the plaintiff must identify its trade secrets with specificity.²¹⁸ The following categories of information have been held not to be trade secrets: "Reasonable measures" to protect secrecy of the information are required,

²¹⁸ *Therapeutics LLC v. Beatty*, 354 F. Supp. 3d 957, 967 (D. Minn. 2018); *Cambria Co. LLC v. Schumann*, No. 19-CV-3145, 2020 U.S. Dist. LEXIS 11373, *10 (D. Minn. Jan. 23, 2020) (denying preliminary injunction where trade secrets were not clearly defined and the plaintiff did not allege that the defendant physically took information from its former employer); *CH Bus Sales*, 2019 U.S. Dist. LEXIS 46093, *22-23 (D. Minn. Mar. 20, 2019) (stating that, post-*Twombly* and *Iqbal*, a plaintiff must describe trade secrets with more than conclusory statements and with sufficient information to infer more than a possibility of misconduct.); *see also Cambria Co. LLC v. Schumann*, No. 19-CV-3145 (NEB/TNL) 2020 U.S. Dist. LEXIS 11373, *10 (D. Minn. Jan. 23, 2020) (denying preliminary injunction where trade secrets are not clearly defined and the plaintiff does not allege that the defendant took any physical information from his employer); *Wilson v. Corning, Inc.*, 171 F. Supp. 3d 869, 882-83 (D. Minn. 2016); *WEG Elec. Corp. v. Pethers*, Civ. No. 16-47, 2016 U.S. Dist. LEXIS 49208, 6 (D. Minn. 2016) (lack of specificity weakens claim); *Loftness Specialized Farm Equip. Inc. v. Twiestmeyer*, Civ. No. 11-1506 (DWF/TNL), 2012 WL 1247232, *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, *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); *Hypred S.A. & A & L Labs., Inc. v. Pochard*, Civ. No. 04-2773, 2004 U.S. Dist. LEXIS 11293, *12 (D. Minn. Jun. 18, 2004) (dissolving temporary restraining order where plaintiff failed to specify trade secrets beyond stating that they were "dealer information," "product formulation and manufacturing secrets").

but the statutes generally do not specifically define what efforts are “reasonable.” The mere “intention to keep material confidential is not enough to confer trade secret protection,” a party must take concrete and tangible measures to ensure that the information remain secret.²¹⁹

1. Customer Lists and Related Information

Although it comes as a surprise to many business people, a company’s customer list usually is not a trade secret.²²⁰ The primary reason for denying trade secret status to customer lists is that the identity of customers is readily ascertainable and often lose their value over a short period of time.²²¹ Courts are also reticent to deem information provided by customers regarding the customer’s needs and orders.²²² An underlying rationale is that courts do not want to create backdoor non-competes through the trade secret statute.²²³ Additionally, there is a strong public interest in preserving competition.²²⁴

In limited circumstances, a customer list might be protected. A customer list that contains more than bare customer names and includes a

²¹⁹ *Nw. Airlines v. Am. Airlines*, 853 F. Supp. 1110, 1115 (D. Minn. 1994); *Denson Int’l Ltd. v. Liberty Diversified Int’l, Inc.*, Civ. No. 12-3109, 2015 U.S. Dist. LEXIS 116092, *15 (D. Minn. Sept. 1, 2015) (denying injunction where plaintiff argued that “the importance of confidentiality was widely assumed” in the business community without taking specific steps to designate the information as confidential).

²²⁰ *Katch, LLC v. Sweetser*, 143 F. Supp. 3d 854, 868-69 (D. Minn. 2016) (identity of key customers and pricing that can be determined by asking customers is not a trade secret); *see also 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)); *Harley Auto. Group, Inc. v. AP Supply, Inc.*, Civ. No. 12-1110, 2013 WL 6801221, *7 (D. Minn. Dec. 23, 2013); *Equus Computer Sys. v. N. Computer Sys., Inc.*, Civ. No. 01-657, 2002 WL 1634334, *4 (D. Minn. July 22, 2002); *Universal Hosp. Servs., Inc. v. Henderson*, Civ. No. 02-951, 2002 WL 1023147, *4 (D. Minn. May 20, 2002); *Oberfoell v. Kyte*, No. A17-0575, 2018 Minn. App. Unpub. LEXIS 74, *21-22 (Minn. Ct. App. Jan. 22, 2018); *Wells Fargo Ins. Servs. USA v. King*, No. 15-CV-4378, 2016 U.S. Dist. LEXIS 8279, *22-23 (D. Minn. Jan. 25, 2016).

²²¹ *Wells Fargo Ins. Servs. USA*, 2016 U.S. Dist. LEXIS 8279 at *23; *Equus*, 2002 WL 1634334, *3-4; *Associated Med. Ins. Agents, L.L.C. v. G.E. Med. Protective Co.*, No. A03-1373, 2004 WL 615002, *4 (Minn. Ct. App. Mar. 30, 2004).

²²² *Tension Envelope Corp. v. JBM Envelope Co.*, 876 F.3d 1112, 1122 (8th Cir. 2017) (applying Missouri trade circuit law).

²²³ *Equus*, 2002 WL 1634334, *5 (citing *Int’l. Bus. Mach. Corp. v. Seagate Tech., Inc.*, 941 F. Supp. 98, 101 (D. Minn. 1992)); *WEG Elec. Corp.*, 2016 U.S. Dist. LEXIS 49208 at *7.

²²⁴ *Lasermaster*, 931 F. Supp. at 637.

customer's buying, pricing and payment history may be considered a trade secret.²²⁵ Moreover, if the customer list segregates customers into high-volume or high-margin categories, the list might be protected as a trade secret.²²⁶ 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.²²⁷ An effective way for a business to protect customer information, however, is to enter into a valid non-competition or non-disclosure agreement.

2. General Knowledge in the Industry

Information that is not known to the general public, but widely known within an industry, is not a trade secret.²²⁸ For instance, an executive's knowledge of contact people within a given industry is not a trade secret.²²⁹

3. Personal Expertise and General Business Information

General marketing intelligence, pricing structures, business expertise, or business plans do not constitute trade secrets.²³⁰ Generally, courts will not protect broad categories of business information.

²²⁵ *Equus*, 2002 WL 1634334, *4; *Dexon Computer, Inc. v. Modern Enter. Solutions*, No. A16-0010, 2016 Minn. App. Unpub. LEXIS 741, *11-12 (Minn. Ct. App. Aug. 1, 2016) (affirming temporary restraining order where the information contained information on more than 10,000 potential customers along with networking, research and sales information about specific customers).

²²⁶ *Equus*, 2002 WL 1634334, *4.

²²⁷ *Id.*; *Associated Med.*, 2004 WL 615002, *4.

²²⁸ *Fox Sports Net N., LLC v. Minn. Twins P'ship*, 319 F.3d 329, 336 (8th Cir. 2003).

²²⁹ *Id.*

²³⁰ *Electro-Craft*, 332 N.W.2d at 900 ("The law of trade secrets will not protect talent or expertise, only secret information."); *Newleaf Designs*, 168 F. Supp. 2d at 1044; *Seagate Tech.*, 941 F. Supp. at 100; *Luigino's, Inc. v. Peterson*, 317 F.3d 909, 912 (8th Cir. 2003); *Integrated Process Sols., Inc. v. Lanix LLC*, No. 19-CV-567, 2019 U.S. Dist. LEXIS 43808, *12 (D. Minn. Mar. 18, 2019) (holding that statement that trade secrets include financial records; bidding information; and standards, blocks, and software is insufficiently precise to identify trade secret); *Goodbye Vanilla, LLC v. Aimia Proprietary Loyalty United States, Inc.*, 304 F. Supp. 3d 815 (D. Minn. 2018) (granting summary judgment where plaintiff e-mail "containing quotations and recommendations" rises to the level of trade secrets); *WEG Elec. Corp.*, 2016 U.S. Dist. LEXIS 49208 at *5 ("[C]ustomer, inventory, and pricing lists, as well as documents containing other institutional knowledge and operation strategies - generally do not constitute trade

4. Variations on a Widely Used Process

Variations on a widely used process do not constitute trade secrets.²³¹ Thus, one court refused to grant trade secret protection to a computer system that merely combined well-known subsystems.²³²

5. Obsolete Information

It should come as no surprise that obsolete information is not considered a trade secret because it has no economic value.²³³ The trick, however, is determining when information becomes 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.²³⁴ In another case, information regarding business strategies that was six months old was considered obsolete and therefore no longer a trade secret.²³⁵

6. Easily Reverse-Engineered Information

secrets"); *Denson Int'l Ltd.*, 2015 U.S. Dist. LEXIS 116092 (granting summary judgement where alleged trade secrets included information "about our employment, our staff levels, our staff levels, our salaries, our overhead, our expenses, . . . [and] our profit margins" because the information was general and trade secrets were not specifically identified); *Excel Mfg. v. Wondrow*, No. A15-1325, 2016 Minn. App. Unpub. LEXIS 385, *11-12 (Minn. Ct. App. Apr. 18, 2016) (holding that "laundry list" of items such as "design prints, product specifications, pricing information, marketing plans and potential customers" are "general categories of information that do not qualify as trade secrets."). Keep in mind that business information such as "detailed customer pricing data" and "sales analysis and strategies" might constitute trade secret if a company takes "significant time, effort, and expense" to maintain its confidentiality, it is not knowable through proper means, and value is derived from its privacy. *See, e.g., Deluxe Fin. Servs., LLC v. Shaw*, Civ. No. 16-3065, 2017 U.S. Dist. LEXIS 122795, 7-8 (D. Minn. Aug. 3, 2017) (denying motion to dismiss where trade secrets were sufficiently alleged in complaint). Furthermore, courts will often give plaintiffs more leeway at the motion to dismiss stage at the outset of the litigation. *Management Registry v. A.W. Cos.*, No. 0:17-cv-05009, 2019 WL 7838280, 2019 U.S. Dist. LEXIS 226063, *28-29 (D. Minn. Sept. 12, 2019); *TE Connectivity Networks, Inc.*, 2013 U.S. Dist. LEXIS 180392 at *8-10 (denying motion to dismiss where "somewhat vague" allegations were sufficient to state a trade secrets claim "when the allegations are viewed as a whole").

²³¹ *Electro-Craft*, 332 N.W.2d at 899.

²³² *Id.* (citing *Jostens, Inc. v. Nat'l Computer Sys.*, 318 N.W.2d 691, 700-01 (Minn. 1982)).

²³³ *Fox Sports Net*, 319 F.3d at 336; *WEG Elec. Corp.*, 2016 U.S. Dist. LEXIS 49208 at *7; *Katch, LLC*, 143 F. Supp. 3d 854.

²³⁴ *Id.*

²³⁵ *Lexis-Nexis v. Beer*, 41 F. Supp. 2d 950, 959 (D. Minn. 1999).

If an item is available in the marketplace and easily reverse-engineered, then the item does not constitute a trade secret.²³⁶

7. Publicly Filed Information

Once information is disclosed in a patent application, it loses its trade secret status.²³⁷ Likewise, other information that is submitted to a public entity, such as in a public government bid, may lose trade secret protection. Thus, it is important to determine whether information submitted to a public entity falls within an exception to state or federal open-records laws and, if so, to follow the procedures to confidentially submit the information.

PRACTICE POINTER: One of the dilemmas a plaintiff seeks in any litigation and particularly a trade secret litigation is that the litigation itself might result in disclosure of the trade secret, particularly as federal courts are requiring parties to plead and identify the elements with a greater degree of specificity.²³⁸ It is therefore critical for parties to establish procedures, such as protective orders, confidentiality designations, and filing documents under seal to prevent such disclosures. The federal statute instructs courts to “enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of the trade secrets” consistent with the state and federal rules of procedure and evidence, and other related laws.²³⁹

III. MISAPPROPRIATION DEFINED

²³⁶ *Electro-Craft*, 332 N.W.2d at 899.

²³⁷ *Coenco, Inc. v. Coenco Sales, Inc.*, 940 F.2d 1176, 1179 n.3 (8th Cir. 1991); *Wilson v. Corning, Inc.*, 171 F. Supp. 3d 869, 882 (D. Minn. 2016) (a claim for a trade secret cannot be made for misappropriation after the trade secret is published in a patent application); *Accent Packaging, Inc. v. Leggett & Platt, Inc.*, 707 F.3d 1318, 1329 (Fed. Cir. 2013) (“As a matter of law, any specifications and tolerances disclosed in or ascertainable from the asserted patents became publicly available . . . when the . . . patent application was published and, as such, could not constitute a trade secret [a few months later] when [the defendant] is alleged to have engaged in misappropriation.”)

²³⁸ See *infra* note 22.

²³⁹ 18 U.S.C. § 1835.

The trade secret statutes defining misappropriation three ways: acquisition through improper means, disclosure, or use.²⁴⁰ A party asserting a claim for misappropriation has the burden to prove both that the information at issue is a trade secret and that the defendant misappropriated it.²⁴¹

A. Improper Acquisition

The trade secret statutes prohibit the acquisition of a trade secret by improper means such as “theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means.”²⁴² Improper means also likely includes lawful conduct which is improper under the circumstances; for example, an airplane overflight used as aerial reconnaissance to determine the competitor's plant layout during construction of the plant.²⁴³ A party that later acquires a trade secret is also liable if it knows or has reason to know that the trade secret was initially acquired by improper means.²⁴⁴

Importantly, it is not improper to learn a trade secret through reverse engineering, independent development, or other lawful means.²⁴⁵ Reverse engineering is starting with the known product and working backward to determine the method by which it was developed.²⁴⁶ Independent derivation occurs with another party develops the product or process from its own independent efforts. Finally, a party may acquire a trade secret through legitimate means such as through permission and voluntary sharing.

B. Disclosure

²⁴⁰ 18 U.S.C. § 1839(5); *Electro-Craft*, 332 N.W.2d at 897; *Goodbye Vanilla, LLC*, 304 F. Supp. 3d at 820. The statute of limitations for misappropriation of trade secrets under federal and Minnesota law is three years. 18 U.S.C. § 1836(d); MINN. STAT. § 325C.06.

²⁴¹ *CPI Card Grp., Inc. v. Dwyer*, 294 F. Supp. 3d 791, 807 (D. Minn. 2018); *Widmark v. Northrup King Co.*, 530 N.W.2d 588, 592 (Minn. Ct. App. 1995).

²⁴² 18 U.S.C. § 1839(6)(A).

²⁴³ Unif. Trade Secrets Act § 1, com.

²⁴⁴ 18 U.S.C. § 1839(5)(A).

²⁴⁵ 18 U.S.C. § 1839(6).

²⁴⁶ *Kewanee v. Bicon*, 416 U.S. 470, 476 (1974); David S. Almeling, *et al. A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZ. L. REV. 291, 324 (2009/10).

Misappropriation also happens when a non-owner discloses another's trade secrets without authorization.²⁴⁷ In limited circumstances, a trade secret owner can successfully assert that a departing employee will inevitably disclose trade secrets if they move to a similar position in another company.²⁴⁸ In jurisdictions where the inevitable disclosure theory is available, the plaintiff must meet a high bar to show that there is a high degree of probability that the other party will disclose the trade secret information.²⁴⁹

C. Use

While the statutes focus on improper acquisition or disclosure of trade secrets, courts will also examine whether a party actually uses or intends to use the trade secret information. For instance, evidence that a departing employee intended to take his former employer's protected information may be insufficient to show misappropriation if there is no additional evidence that the employee actually took or used the information.²⁵⁰

IV. POTENTIAL EXPOSURE

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.

²⁴⁷ 18 U.S.C. 1832(a)(2); MINN. STAT. §325C.01, subd. 3(ii).

²⁴⁸ 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, 2013 WL 9851104, *6 (D. Minn. Dec. 11, 2013); *see also* *Prime Therapeutics LLC v. Beatty*, 354 F.Supp.3d 957, 968-72 (D. Minn. 2018) (denying injunctive relief where plaintiff failed to sufficient evidence to meet the very high bar to show inevitable disclosure); *United Prods. Corp. of Am. v. Cederstrom*, No. A05-1688, 2006 Minn. App. Unpub. LEXIS 594, *14 (D. Minn. Jun. 6, 2006) (same); *Katch, LLC*, 143 F. Supp. 3d at 872-73 (same); *Mid-Am. Bus. Sys. v. Sanderson*, Civ. No. 17-3876, 2017 U.S. Dist. LEXIS 166463, *20-21 (D. Minn. Oct. 6, 2017) (same).

²⁴⁹ *See id.* *Prime Therapeutics LLC*, 354 F.Supp.3d at 968-72.

²⁵⁰ *Integrated Process Sols.*, 2019 U.S. Dist. LEXIS 43808 at *13 (denying injunction).

A. Money Damages

A plaintiff can recover both its lost profits and for any unjust enrichment the defendant received from the theft.²⁵¹ In lieu of damages measured by other means, a court may impose a reasonable royalty for the defendant's use of the trade secret.²⁵²

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.²⁵³ 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, the 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

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 where the plaintiff can prove likelihood of success on the merits and irreparable harm.²⁵⁴ In our hypothetical scenario, the plaintiff would be entitled to an injunction preventing the defendant from selling the software.

²⁵¹ 18 U.S.C. § 1836(b)(3(B)(i)(II)); *Children's Broad. Corp. v. The Walt Disney Co.*, 357 F.3d 860, 865 (8th Cir. 2004) (citing MINN. STAT. § 325C.03(a)).

²⁵² 18 U.S.C. § 1836(b)(3(B)(ii)); MINN. STAT. § 325C.03(a).

²⁵³ MINN. STAT. § 325C.03.

²⁵⁴ 18 U.S.C. § 1836(b)(3(A)); MINN. STAT. § 325C.02. Note, that while irreparable harm was often associated with trade secret misappropriation, recent courts have found that against a presumption of irreparable harm. *See MPAY Inc. v. Erie Custom Computer Applications*, 970 F.3d 1010, 1019-21 (8th Cir. 2020).

An injunction may not be issued where, even if there is evidence that a former employee possessed or possesses trade secrets, there is no evidence that the employee will disclose or use that information, particularly where employees commit to not using or disclosing the information.²⁵⁵

In situations where a former employee takes significant proprietary information, computers and data, Minnesota courts may issue injunctive relief ordering the former employee to return all information, prohibiting further disclosure or communication regarding the trade secrets, using or copying trade secrets, making all computers and electronic devices available for computer forensic duplication and examination, and submitting an affidavit regarding all destroyed information.²⁵⁶

The length of the injunction is determined by the period of time that would be required for independent development of the trade secret.²⁵⁷ The time period of the injunction can be extended to eliminate any commercial advantage that a defendant derived from the misappropriation.²⁵⁸

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.²⁵⁹ The Eighth Circuit upheld the district court's decision to permanently enjoin the defendant from producing estrogen.²⁶⁰ 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

²⁵⁵ *Midwest Sign & Screen Printing Supply Co. v. Robert Dalpe & Laird Plastics, Inc.*, 386 F. Supp. 3d 1037, 1053-54 (D. Minn. 2019) (denying injunction where employee forwarded confidential information to their home email because there was no evidence that the employee would subsequently use or disclose the information); *CPI Card Grp.*, 294 F. Supp. 3d at 804; *Mid-Am. Bus. Sys.*, 2017 U.S. Dist. LEXIS 166463 (denying trade secrets injunction where the plaintiff merely speculates that the defendant will use information).

²⁵⁶ *Advanced Control Tech., Inc. v. Iversen*, Civ. No. 19-1608, 2019 WL 3037089, 2019 U.S. Dist. LEXIS 117355, *2-5 (D. Minn. Jul. 3, 2019).

²⁵⁷ *Wyeth*, 2003 WL 22282371, *27 (citing *Surgidev*, 648 F. Supp. at 696).

²⁵⁸ 18 U.S.C. § 1836(b)(3)(B)(i)(II); MINN. STAT. § 325C.02(a).

²⁵⁹ *Wyeth*, 395 F.3d at 899.

²⁶⁰ *Id.* at 903.

undertake future research into developing an alternative process without relying on the misappropriated trade secrets.²⁶¹ The injunction put the defendant out of business.

PRACTICE POINTER: 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 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 and Malicious Risks Double Damages

In addition to lost profits, unjust enrichment, and reasonable royalties, a defendant whose misappropriation was willful and malicious will be liable for the plaintiff's attorneys' fees as well as exemplary damages up to twice the value of actual damages.²⁶² A trio of trade secret cases have identified the following conduct as willful and malicious:²⁶³

- 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.

²⁶¹ *Id.*

²⁶² 18 U.S.C. § 1836(b)(3)(C-D); MINN. STAT. §§ 325C.03(b) & 325C.04.

²⁶³ *Scott Equip. Co.*, 2003 WL 21804868, *3 (management knowledge); *K-Sun Corp.*, 1998 WL 422182, *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).

PRACTICE POINTER: 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 also makes juries, judges, and arbitrators mad, which leads to findings of willful and malicious misappropriation and big damages.²⁶⁴

D. Bad Faith Adds Attorney's Fees

Attorney's 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.²⁶⁵ 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.²⁶⁶ However, courts have held that a trade secret claim is not brought in bad-faith if it survives summary judgment²⁶⁷ or does not merit sanctions.⁵¹

PRACTICE POINTER: If there may be the potential for an award of fees for malicious/willful misappropriation or bad faith in bringing the claim, legal counsel should take care to differentiate the fees incurred to litigate the trade secret claim, verses other claims in the lawsuit.

²⁶⁴ *In re Adegoke*, 632 B.R. 154 (N.D. Ill. 2021) (citing cases where courts infer misappropriation from spoliation of evidence).

²⁶⁵ 18 U.S.C. 1836(b)(3)(D); MINN. STAT. § 325C.04.

²⁶⁶ *Norwood Operating Co. v. Beacon Promotions, Inc.*, Civ. No. 04-1390, 2006 WL 3103154, *1-2 (D. Minn. Oct. 31, 2006).

²⁶⁷ *Id.* *3; *Wixon Jewelers, Inc. v. Aurora Jewelry Designs*, No. C0-01-2149, 2002 WL 1327014, *2 (Minn. Ct. App. June 18, 2002); *Weaver v. Iverson*, No. A12-0354, 2012 WL 3641358, *2 (Minn. Ct. App. Aug. 27, 2012).

COMMON CONTEXTS IN WHICH 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.²⁶⁸ The threat of misappropriation is established if the party seeking the injunction can show there is "a high degree of probability of inevitable disclosure."²⁶⁹ A party can establish actual misappropriation either by direct or circumstantial evidence.²⁷⁰

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 them. The new employer might be held liable for misappropriation or theories of vicarious liability.²⁷¹ Moreover, even if a company has not used the information, it might still be subject to an injunction under the inevitable disclosure doctrine.²⁷² There are also a host of other companion claims that departing employees and their new employers should have on their radar screen including, for instance, tortious interference with business relationships, breach of fiduciary duty, and breach of duties of confidentiality and loyalty.²⁷³

²⁶⁸ 18 U.S.C. 1836(b)(3)(A); MINN. STAT. § 325C.02.

²⁶⁹ *Lexis-Nexis*, 41 F. Supp. 2d at 958 (citations omitted).

²⁷⁰ *Wyeth*, 2003 WL 22282371, *21 (citing *Pioneer Hi-Bred Int'l v. Holden Found. Seeds, Inc.*, 35 F.3d 1226, 1239 (8th Cir. 1994)).

²⁷¹ *Deluxe Fin. Servs.*, 2017 U.S. Dist. LEXIS 122795 at *10-11.

²⁷² *Lexis-Nexis*, 41 F. Supp. 2d at 959.

²⁷³ See, e.g., *Bison Advisors*, 2016 U.S. Dist. LEXIS 88307; *Mid-Am. Bus. Sys.*, 2017 U.S. Dist. LEXIS 166463, 2017; *Nilfisk, Inc. v. Liss*, No. 17-cv-1902, 2017 WL 7370059, 2017 U.S. Dist. LEXIS 220970 (D. Minn. Jun. 15, 2017).

B. Business Acquisitions and 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.²⁷⁴ Other Minnesota cases illustrate that the bad feelings that often arise from a failed acquisition can give rise to trade secret claims.²⁷⁵

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 and 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. COMPANY ACTIONS TO AVOID TRADE SECRET CLAIMS

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 a company's core business operations or research and development. The screening should focus on the employee's actual technical knowledge as

²⁷⁴ *K-Sun*, 1998 WL 422182, *1-4.

²⁷⁵ See, e.g., *Protégé Biomedical, LLC v. Z-Medica, LLC*, 394 F. Supp. 3d 924, 939-40 (D. Minn. 2019); *Luigino 's*, 2002 WL 122389.

opposed to general knowledge or skills that the employee gained at his previous job.²⁷⁶

New employees should be instructed not to disclose or use a former employer's trade secret information in connection with their employment with the company. Additionally, new employees should be required to attest something akin 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

²⁷⁶ *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); *Prime Therapeutics LLC*, 354 F.Supp.3d at 972 (denying preliminary injunction where departing employee was forthright about transition to new employer and there was no evidence that employee took documents containing trade secret information with her); *Reliastar Life Ins. Co. v. KMG Am. Corp.*, No. A05-2079, 2006 Minn. App. Unpub. LEXIS 1018, 2006 WL 2529760, *5 (Minn. Ct. App. Sept. 5, 2006) ("[m]erely possessing trade secrets and holding a comparable position with a competitor does not justify an injunction" (citation and quotations omitted)).

work for their employer.²⁷⁷ 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.²⁷⁸ 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 a 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. When a party accused of misappropriation, that party may be able to weaken an alleged

²⁷⁷ See, e.g., *Mid-Am. Bus. Sys.*, 2017 U.S. Dist. LEXIS 166463 (denying temporary restraining order where there is not clear evidence that the departing employee is likely to use information in new position).

²⁷⁸ 18 U.S.C. § 1839, subd. 5; MINN. STAT. § 325C.01, subd. 3.

misappropriation claim by committing to not use or disclose particular information.²⁷⁹

VI. COMPANY ACTIONS PROTECT ITS TRADE SECRETS

A trade secret owner must take *reasonable measures* to protect secrecy.²⁸⁰ While the statute does not define reasonableness, courts will evaluate the particular trade secret and circumstances of the business.²⁸¹ 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."²⁸²

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.

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.

Companies should, at minimum, conduct an audit of their intellectual property and trade secrets. They need to identify their trade secret information, implement procedures to reasonably protect the secrecy of the information, and assess and manage potential risks of misappropriation.

²⁷⁹ Virtual Radiologic Corp. v. Rabern, No. 20-CV-0445, 2020 WL 1061465, 2020 U.S. Dist. LEXIS 37746, *9-10 (D. Minn. Mar. 5, 2020) (denying preliminary injunction where defendant hired outside firm to conduct forensic examination of computer and email accounts to confirm that it did not possess secret information).

²⁸⁰ 18 U.S.C. 1839(3)(A); MINN. STAT. § 325C.01, subd. 5.

²⁸¹ *Id.*

²⁸² *Lasermaster*, 931 F. Supp. at 635.

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.²⁸³ Remember that the defense in a trade secret case will focus on the defendant 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.²⁸⁴ It may be helpful to start with locking down protection for the company's crown jewels. Specifically identify and protect the core trade secrets, and then strategically assess whether and how to protect secondary and tertiary information.

B. Stamp 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."²⁸⁵ Moreover, a business must make sure that it follows its own procedures, or risk losing trade secret status. In one case, a business required the marking of trade secret documents as "confidential" but failed to stamp the information it sought to protect.²⁸⁶

²⁸³ *Lexis-Nexis*, 41 F. Supp. 2d at 959.

²⁸⁴ *See, e.g., Menzies Aviation (USA), Inc. v. Wilcox*, 978 F. Supp. 2d 983, 995 (D. Minn. 2013).

²⁸⁵ *CPI Card Grp., Inc.*, 294 F. Supp. 3d at 809 (denying injunction where alleged trade secrets were not marked as "confidential" or were not specifically defined); *AvidAir Helicopter Supply, Inc.*, 663 F.3d at 974 (citing *Wyeth*, 395 F.3d at 899-900 & n.4); *Oberfoell*, 2018 Minn. App. Unpub. LEXIS 74 at *9 (holding that secrecy requirement was not met where alleged trade secrets were not maintained in password protected systems or marked as confidential);

²⁸⁶ *Lexis-Nexis*, 41 F. Supp. 2d at 959.

The court found that the business's failure to stamp the documents indicated that it had failed to take reasonable measures to protect them.²⁸⁷

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.²⁸⁸

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.²⁸⁹ 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.²⁹⁰ 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 pursuing claims against employees who violate their non-disclosure obligations.²⁹¹ Moreover, where a company has a non-disclosure agreement, those contractual duties will define whether a misappropriation has taken place.²⁹² Thus, a company will want to

²⁸⁷ *Id.*

²⁸⁸ *Electro-Craft*, 332 N.W.2d at 902.

²⁸⁹ *Relco, LLC v. Keller*, No. A13-1633, 2014 WL 2921895, *6 (Minn. Ct. App. June 30, 2014) (citing *Cherne Indus., Inc. v. Grounds & Assocs., Inc.*, 278 N.W.2d 81, 90 (Minn. 1979)).

²⁹⁰ *Coyne's & Co., Inc. v. Enesco, LLC*, Civ. No. 07-4095, 2010 WL 3269977, *16 (D. Minn. Aug. 16, 2010); *Storage Tech. Corp. v. Cisco Sys., Inc.*, Civ. No. 00-2253, 2003 WL 22231544, *7 (D. Minn. Sept. 25, 2003) (citing *Electro-Craft*, 332 N.W.2d at 902).

²⁹¹ *See Id.*

²⁹² *Coyne's & Co.*, 2010 WL 3269977, *16.

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. Noncompetition 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 noncompetition agreement prior to commencing employment. If an existing employee is asked to sign a noncompetition 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,

North Dakota, Montana)²⁹³ 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.²⁹⁴ While one federal court has adopted this approach,²⁹⁵ 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.²⁹⁶ 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.²⁹⁷

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

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

²⁹³ 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.”); MCA §28-2-704 and 705; N.D.C.C. § 9-08-06.

²⁹⁴ See, e.g., *Fifield v. Premier Dealer Servs., Inc.*, 993 N.E.2d 938, 943 (Ill. App. Ct. 2013) (collecting cases).

²⁹⁵ *Instant Tech., LLC v. DeFazio*, No. 12 C 491, 2014 WL 1759184, *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.”).

²⁹⁶ *Cumulus Radio Corp. v. Olson*, No. 15-CV-1067, 2015 WL 643345, *4 (C.D. Ill. Feb. 13, 2015) (“[T]he 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, *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.”).

²⁹⁷ *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).

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.²⁹⁸

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.²⁹⁹ Failure to keep sensitive drawings or documents in a central and locked location will often defeat a trade secret claim.³⁰⁰

Similarly, restricting visitors to sensitive areas of a plant or facility will protect trade secrets.³⁰¹ 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.³⁰² Failure to restrict visitor access can defeat a trade secret claim.³⁰³ Securing entrances to buildings and certain sensitive areas within facilities is also important.

PRACTICE POINTER: Pride goes 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, company agents must be careful not to disclose trade secrets during these events. A company should segregate any sensitive processes or technology from a plant tour and carefully monitor employee presentations.³⁰⁴

²⁹⁸ *Electro-Craft*, 332 N.W.2d at 903.

²⁹⁹ *Surgidev*, 648 F. Supp. at 693-94 (citations omitted).

³⁰⁰ *Electro-Craft*, 332 N.W.2d at 902.

³⁰¹ *Surgidev*, 648 F. Supp. at 693.

³⁰² *Id.*; *Electro-Craft*, 332 N.W.2d at 902.

³⁰³ *Surgidev*, 648 F. Supp. at 693. 84 *Electro-Craft*, 332 N.W.2d at 902 85 *Id.*

³⁰⁴ Defendants often assert that information that is available through tours and public presentations loses its trade secret status. *See, e.g.,* ACG, Inc. v. Bailageron, No. CV10601844S, 2011 Conn. Super. LEXIS 549. *45-48 (Sup. Ct. Conn. Mar. 9, 2011) (finding that company failed to take reasonable measures to protect secrecy of information when it gave tours of its facilities to competitors without taking additional confidentiality precautions); TWR Serv. Corp. v. Peterson, 2021 IL App (2d) 210208-U (Ill. App. Ct., 2nd Dist., *88-90 (Dec. 2, 2021).

F. Digital Security

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.³⁰⁵ 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.

G. Publication Policies

The policies may include a screening process for all outgoing publications and speeches to ensure that no confidential information is disseminated.³⁰⁶ 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.

³⁰⁵ *Dexon Computer, Inc.*, 2016 Minn. App. Unpub. LEXIS 741 at *13-14. Password protections and confidentiality agreements are not, by themselves, sufficient to show reasonable efforts to maintain secrecy.

³⁰⁶ *Id.* at 901-02.

H. 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.³⁰⁷

I. 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.³⁰⁸

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.

J. Employee and Vendor Training and Follow-Through

Policies only go so far - employees and third parties need to be trained on the policies and know what steps they need to take to protect confidential information. Failure to take these simple steps - which can fall outside basic corporate training - has resulted in failed litigation and lost protections. Likewise, trade secret protections may be lost if employees routinely disregard confidentiality policies and security measures.³⁰⁹

³⁰⁷ *Surgidev*, 648 F. Supp. at 693.

³⁰⁸ *Id.* at 694.

³⁰⁹ *Berkley Risk Adm'rs Co.*, 2016 U.S. Dist. LEXIS 113421 (evidence that employees emailed confidential information to their personal email accounts cuts against requirement to reasonably protect trade secrets); *Lexis-Nexis*, 41 F. Supp. 2d at 959 (finding that policies which “were frequently disregarded in practice” raised a substantial question as to whether plaintiff made reasonable efforts to maintain secrecy).

K. Establish a Trade Secret Team – Implement Continual Improvement

Problems arise when no one within a company has overall responsibility for protecting trade secrets and other confidential information. Courts may look unfavorably on companies that fail to put a person or group in charge of protecting trade secrets. Consider establishing a cross-functional team with broad representation to establish trade secret policies and ensure that those policies are being followed.

Companies are also well-served to develop a plan to respond in the event of a breach. This may include vetting legal counsel who can respond on a dime.

VII. COMMON COMPANION CLAIMS

The Federal Defend Trade Secrets Act of 2016 (“FDTSA”) does not affect “contractual remedies, whether or not based upon misappropriation of a trade secret” or “other civil remedies that are not based upon misappropriation of a trade secret.”³¹⁰ The MTSA, meanwhile, displaces tort claims that do not allege additional factual allegations beyond the misappropriation of trade secrets or seek remedies beyond the MTSA.³¹¹ Common companion claims include, for instance, breach of fiduciary duties and the duty of loyalty, tortious interference of business relations, and theft.

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.

³¹⁰ MINN. STAT. § 325C.07

³¹¹ *SL Montevideo Tech., Inc. v. Eaton Aerospace, LLC*, 292 F. Supp. 2d 1173, 1179 (D. Minn. 2003); MINN. STAT. § 325C.07(a) (stating that the Act “displace[s] conflicting tort, restitutionary, and other law of this state providing civil remedies for misappropriation of a trade secret”); *Micro Display Sys., Inc. v. Axtel, Inc.*, 699 F. Supp. 202, 205 (D. Minn. 1988) (“To the extent a cause of action exists in the commercial area not dependent on trade secrets, that cause continues to exist.”).

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 accessor is not entitled so to obtain or alter.”³¹²

However, “without authorization” is not defined by the statute. 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.³¹³ 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.³¹⁴

VIII. 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

³¹² 18 U.S.C.A. § 1030(a)(4).

³¹³ See *Micro Display Sys.* 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).

³¹⁴ *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).”).

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.