

THE SECRETS OF TRADE SECRETS: PROTECTING YOUR COMPANY'S TRADE SECRETS AND PROTECTING YOUR COMPANY AGAINST TRADE SECRET CLAIMS

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 an injunction shutting a business down 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

¹ Minn. Stat. § 325C.01 (West 2004).

² Minn. Stat. § 325C.01 (West 2004); *Electro-Craft Corp. v. Controlled Motion, Inc.*, 332 NW.2d 890, 899-902 (Minn. 1983).

³ *Electro-Craft* at 899.

⁴ *Surgidev Corp. v. Eye Tech, Inc.*, 648 F.Supp 661, 688 (D. Minn. 1986) (MacLaughlin, J.).

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

Second, the information must gain independent economic value from its secrecy.⁷ “Generally, if substantial time and money would be required of a competitor to develop the same information, that information has economic value.”⁸ 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.⁹

Third, a plaintiff must show that it made reasonable efforts to maintain the secrecy of the trade secret.¹⁰ Trade secret law “does not require the maintenance of absolute secrecy; only partial secrecy or qualified secrecy has been required under the common law.”¹¹ For instance, a party “acted reasonably to maintain secrecy by requiring a confidentiality agreement for [the defendant] and marking its documents and files as confidential.”¹²

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

⁵ *Scott Equip. Co. v. Stedman Mach. Co.*, 2003 WL 21804868, *2 (D. Minn. July 31, 2003) (Ericksen, J.).

⁶ *Surgidev* at 689 (citing *Electro-Craft*).

⁷ *Electro-Craft* at 900.

⁸ *Surgidev* at 692.

⁹ *Wyeth v. Natural Biologies, Inc.*, 2003 WL 22282371, *19 (D. Minn. 2003) (Erickson, J.); *I-Systems, Inc. v. Softwares, Inc.*, 2004 WL 742082, *14 (D. Minn. March 29, 2004) (Tunheim, J.).

¹⁰ *Electro-Craft* at 901.

¹¹ *Surgidev* at 692-3.

¹² *K-Sun Corp. v. Heller Ins., Inc.*, 1998 WL 422182, *3 (Minn. Ct. App. July 28, 1998).

Although it comes as a surprise to many business people, a company's customer list usually is not a trade secret.¹³ The primary reason for denying trade-secret status to customer lists is that the identity of customers is readily ascertainable.¹⁴ An underlying rationale is that courts do not want to create backdoor non-competes through the trade-secret statute.¹⁵ Additionally, there is a strong public interest in preserving competition.¹⁶

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.¹⁷ Moreover, if the customer list segregates customers into high volume or high margin categories, the list might be protected as a trade secret.¹⁸ 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.¹⁹ The best way for a business to protect customer information, however, is to enter into a valid non-compete agreement.

(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.²⁰ For instance, an executive's knowledge of contact people within a given industry is not a trade secret.²¹

¹³ *Equus Computer Sys. v. N. Computer Sys., Inc.*, 2002 WL 1634334, *4 (D. Minn. 2002) (Frank, J.); *Universal Hosp. Servs., Inc. v. Henderson*, 2002 WL 1023147, *4 (D. Minn. 2002) (Kyle, J.); *Newleaf Designs, LLC v. Bestbins Corp.*, 168 F.Supp.2d 1039, 1044 (D. Minn. 2001) (Tunheim, J.); *citing Lasermaster Corp. v. Sentinel Imaging*, 931 F.Supp. 628, 637-8 (D. Minn. 1996) (Davis, J.).

¹⁴ *Equus* at *4; *Associated Medical Ins. Agents, LLC v. G.E. Medical Protective Co.*, 2004 WL 615002, *4 (Minn. Ct. App. 2004).

¹⁵ *Equus* at *5 *citing Intern. Bus. Machs. Corp. v. Seagate Tech., Inc.*, 941 F.Supp. 98, 101 (D. Minn. 1992) (Magnuson, J.).

¹⁶ *Lasermaster*, 931 F.Supp. at 637.

¹⁷ *Equus* at *4.

¹⁸ *Id. citing Surgidev Corp.*, 648 F.Supp. at 683.

¹⁹ *Associated Medical* at *4.

²⁰ *Fox Sports Net N., LLC v. Minnesota Twins Partner*, 319 F.2d 329, 336 (8th Cir. 2003).

²¹ *Id.*

(3) general business information

General marketing intelligence or business plans do not constitute trade secrets.²² Generally, the courts will not protect broad categories of business information.²³

(4) variations on a widely used process

Variations on a widely used process do not constitute trade secrets.²⁴ Thus, a court refused to grant trade secret protection to a computer system that merely combined known subsystems.²⁵

(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.²⁶ 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.²⁷ Likewise, information regarding business strategies that was six months old was held obsolete, and therefore not a trade secret.²⁸

(6) easily reverse-engineered information

If an item is available in the market place and easily reverse-engineered, then the item does not constitute a trade secret.²⁹

²² *Newleaf Designs*, 168 F.Supp.2d at 1044; *Seagate Tech.*, 941 F.Supp. at 100.

²³ *Seagate* at 100.

²⁴ *Electro-Craft*, 332 N.W.2d at 889.

²⁵ *Electro-Craft* at 889 citing *Jostens, Inc. v. Nat'l Computer Sys.*, 318 N.W.2d 691, 701 (Minn. 1982).

²⁶ *Fox Sports*, 319 F.3d at 336.

²⁷ *Id.*

²⁸ *Lexis-Nexis v. Beer*, 41 F.Supp.2d 950, 959 (D. Minn. 1999) (Doty, J.).

²⁹ *Electro-Craft*, 332 N.W.2d at 899.

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 for its lost profits and for any unjust enrichment the defendant received from the theft.³⁰ In lieu of damages measured by other means, the Court may impose a reasonable royalty for the defendant's use of the trade secret.³¹

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.³² The only limitation is that the unjust enrichment damages cannot have been taken into account in determining the plaintiff's losses.³³

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.

³⁰ *Children's Broadcasting Corp. v. Walt Disney Co.*, 357 F.3d 860, 865 (8th Cir. 2004) (citing Minn. Stat. § 325C.03(a)).

³¹ § 325C.03(a).

³² Minn. Stat. § 325C.03 (West 2004).

³³ *Id.*

B. Injunction Malfunction

But 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.³⁴ 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.³⁵ The time period of the injunction can be extended to eliminate any commercial advantage that a defendant derived from the misappropriation.³⁶

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.³⁷ The Eighth Circuit upheld the district court's decision to permanently enjoin the defendant from producing estrogen.³⁸ The Eighth Circuit concluded 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.³⁹ The injunction put the defendant out of business.

³⁴ Minn. Stat. § 325C.02 (West 2004).

³⁵ *Wyeth*, 2003 WL 22282371, *27 citing *Surgidev*, 648 F. Supp. at 696 (citations omitted).

³⁶ Minn. Stat. § 325C.02(a).

³⁷ *Wyeth*, 395 F.3d at 899.

³⁸ *Id.* at 903.

³⁹ *Id.* at 903.

C. Willful & Malicious Is Vicious

In addition to lost profits, unjust enrichment, and reasonable royalties, a defendant can be liable for the plaintiff's attorney fees and for punitive damages up to twice the value of actual damages.⁴⁰ The defendant faces liability for the plaintiff's fees and punitive damages if the misappropriation is willful and malicious.⁴¹

A trio of trade-secret cases have identified the following conduct as willful and malicious:⁴²

- 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.

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.⁴³ The threat of misappropriation is established if the party seeking the injunction can show there is "a high degree of probability of

⁴⁰ Minn. Stat. § 325C.03(b); Minn. Stat. § 325C.04.

⁴¹ *Id.*

⁴² *Scott Equip. Co.* at *3 (management knowledge); *K-Sun Corp. 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).

⁴³ Minn. Stat. § 325C.02.

inevitable disclosure.’⁴⁴ A party can establish actual misappropriation either by direct or circumstantial evidence.⁴⁵

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.⁴⁶

B. Business Acquisitions/Equity Funding

Trade secret claims commonly arise in the context of business acquisitions. The *K-Sun Corp.* case illustrates the dangers that a company can face in the context of an acquisition. Unsuccessful merger negotiations in *K-Sun Corp.* led to the defendant company being liable for attorney fees and punitive damages.⁴⁷ Other Minnesota cases illustrate that the bad feelings that often arise from a failed acquisition can give rise to trade secret claims.⁴⁸

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

⁴⁴ *Lexis-Nexis*, 41 F.Supp.2d at 958 (citations omitted).

⁴⁵ *Wyeth*, 2003 WL 22282371, at *21 citing *Pioneer Hi-Bred Int’l v. Holden Foundation Seeds, Inc.*, 35 F.3d 1226, 1239 (8th Cir. 1994).

⁴⁶ *Lexis-Nexis*, 41 F.Supp.2d at 958 (citations omitted).

⁴⁷ *Id.*, 1998 WL 422182, at *4.

⁴⁸ See *Luigino’s, Inc. v. Peterson*, 2002 WL 122389 (D. Minn. 2002).

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 Trade Secrets?

A trade secret owner must take reasonable measures to protect secrecy.⁴⁹ This reasonableness test is based on the particular circumstances of both the secret itself and the business.⁵⁰ The touchstone test for determining whether a company's security measures are adequate revolves around notice: "If, 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."⁵¹

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 infinite. As a practical matter the care exercised tends to correspond to the economic value of the secret and its nature; some

⁴⁹ Minn. Stat. § 325C.01, subd. 5.

⁵⁰ *Id.*

⁵¹ *Lasermaster Corp.*, 931 F.Supp. at 635.

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 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.⁵² Remember that the defense in a trade-secret case will focus on your company's lapses.

Because these policies' expense is 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.

B. Stamping Out Theft

Courts routinely consider whether documents both used in-house and those circulated to third-parties are marked or stamped as "confidential" or "secret."⁵³ Moreover, a business must make sure that it follows its own procedures, or it risks losing trade-secret status. In one case, a business required that any trade secrets be stamped confidential.⁵⁴ But it had failed to stamp the

⁵² *Lexis-Nexis*, 41 F.Supp.2d at 959.

⁵³ *Wyeth v. Natural Biologics, Inc.*, 395 F.3d 897, 899 (8th Cir. 2005);

⁵⁴ *Lexis-Nexis*, 41 F.Supp.2d at 959.

information it sought to protect.⁵⁵ The court found that the business's failure to stamp the documents indicated that it had failed to take reasonable measures to protect them.⁵⁶

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.⁵⁷

C. Non-Disclosure: An Ounce of Prevention

Although a non-disclosure agreement is an important tool for protecting trade secrets, a non-disclosure alone is not sufficient to protect a company's trade secrets.⁵⁸ 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.⁵⁹

D. 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.

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.⁶⁰ Failure to keep sensitive drawings or documents in a central and locked location will often defeat a trade secret claim.⁶¹

⁵⁵ *Id.*

⁵⁶ *Id.*

⁵⁷ *Electro-Craft Corp.*, 332 N.W.2d at 902.

⁵⁸ *Storage Tech. Corp. v. Cisco Sys., Inc.*, 2003 WL 22231544, *7 (D. Minn. 2003) (Erickson, J.) citing *Electro-Craft*, 332 N.W.2d at 902.

⁵⁹ *Id.*

⁶⁰ *Surgidev Corp. v. Eye Tech. Inc.*, 648 F. Supp 661, 694 (D. Minn. 1986).

⁶¹ *Electro-Craft Corp.*, 332 N.W.2d at 902.

Similarly, restricting visitors to sensitive areas of a plant or facility will protect trade secrets.⁶² 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.⁶³ Failure to restrict visitor access can defeat a trade secret claim.⁶⁴

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.⁶⁵ Physical security measures prevent third party access and are also a way of signaling to employees that certain information is secret.⁶⁶

E. 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 code 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.

F. Publication Policies

The policies may include a screening process for all out-going publications and speeches to ensure that no confidential information is disseminated.⁶⁷ 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,

⁶² *Surgidev Corp.*, 648 F. Supp at 693.

⁶³ *Surgidev Corp.*, 648 F. Supp at 693; *Electro-Craft Corp.*, 332 N.W.2d at 902.

⁶⁴ *Surgidev Corp.*, 648 F. Supp. at 693.

⁶⁵ *Electro-Craft Corp.*, 332 N.W.2d at 902.

⁶⁶ *Electro-Craft Corp.*, 332 N.W.2d at 902

⁶⁷ *Electro-Craft Corp.*, 332 N.W.2d at 901-02.

absent express contractual or statutory protection, trade secret protection will be lost. Adherence to a screening process for all publications can prevent inadvertent disclosure.

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.⁶⁸

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 only for their assigned territory and managers only information for those they supervise.⁶⁹

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.

VI. How To Avoid 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 your company’s core business operations or research and development. The

⁶⁸ *Surgidev Corp.*, 648 F. Supp at 693.

⁶⁹ *Surgidev Corp.*, 648 F. Supp at 694

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.⁷⁰

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.⁷¹ 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.

#3103454\1

⁷⁰ *Lasermaster*, 931 F.Supp. at 636-7 (citation omitted) (“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 cause of his employment . . . the right to use and expand these powers remains his property. . . .”).

⁷¹ Minn. Stat. § 325C.01, subd. 3.