

KEEPING A COMPANY'S CONFIDENCES SECRET: TRADE SECRET ENFORCEMENT UNDER IOWA'S UNIFORM TRADE SECRETS ACT

*Thomas W. Foley**

TABLE OF CONTENTS

| | |
|---|----|
| I. How Is a Trade Secret Violation Established Under Iowa's UTSA? | 4 |
| II. What Is a Trade Secret? | 6 |
| III. What Does It Mean to Derive Economic Value from Not Being Known or Readily Ascertainable Through Proper Means? | 10 |
| IV. Are Customer Lists Trade Secrets? | 17 |
| V. What Efforts Must Be Made to Keep Confidential Information Secret? | 21 |
| VI. How Are Trade Secrets Misappropriated? | 27 |
| VII. Does the UTSA Protect Threatened Misappropriations of Trade Secrets? | 32 |
| VIII. What Can a Company Do When Its Trade Secrets Are, or May Be, Misappropriated? | 37 |
| IX. What Legal Remedies Are Available to a Company When Its Trade Secrets Are Misappropriated? | 38 |
| X. What Is the Future of Iowa Trade Secret Law? | 39 |

* Mr. Foley is a shareholder with Babich Goldman, P.C. in Des Moines, Iowa and is a member of that firm's employment and litigation groups. Prior to December 2009, Mr. Foley was a shareholder with Nyemaster, Goode, West, Hansell & O'Brien, P.C., also in Des Moines, for over twenty five years. Mr. Foley graduated with high distinction from the University of Iowa College of Law in 1985 and received a BBA, with honors, from the University of Iowa in 1982. During his legal career, Mr. Foley has represented individuals and corporations in all types of commercial litigation with an emphasis on employment discrimination, wrongful discharge, noncompete, and other employee departure litigation. Mr. Foley would like to thank the attorneys at the aforementioned law firms who assisted him in preparing this article. He would also like to thank Edmund J. Sease of McKee, Voorhees & Sease for taking the time to review and comment on an earlier draft. His insight and advice was invaluable to the completion of this article.

In April 1990, the Iowa General Assembly passed the Uniform Trade Secrets Act (UTSA), which was later codified as Iowa Code chapter 550.¹ The statute was based on a model act passed by the National Conference of Commissioners on Uniform State Laws in 1979.² At that time, the development of a uniform trade secret law was deemed necessary to bring certainty to the “doubtful and confused status of both common law and statutory remedies” regarding trade secret misappropriation.³ All but four states have since passed some version of the UTSA.⁴

The UTSA defines what information qualifies as trade secrets under Iowa law and includes claims for actual or threatened trade secret misappropriation.⁵ The UTSA is consistent with similar protections that existed before the UTSA was enacted and remain available under Iowa common law.⁶ Broadly stated, the UTSA grants the owner of a trade secret

1. See IOWA CODE § 550 (2009).

2. UNIF. TRADE SECRETS ACT (amended 1985), 14 U.L.A. 529–30 (2005).

3. *Id.* at 531 (quoting Comment, *Theft of Trade Secrets: The Need for a Statutory Solution*, 120 U. PA. L. REV. 378, 380–81 (1971)).

4. ALA. CODE § 8-27-1 (2002); ALASKA STAT. § 45.50.910 (2008); ARIZ. REV. STAT. ANN. § 44-401 (2003); ARK. CODE ANN. § 4-75-601 (2001); CAL. CIV. CODE § 3426 (West 1997); COLO. REV. STAT. § 7-74-101 (2009); CONN. GEN. STAT. ANN. § 35-50 (West 2005); DEL. CODE ANN. tit. 6, § 2001 (2005); FLA. STAT. ANN. § 688.001 (West 2003); GA. CODE ANN. § 10-1-760 (West 2003); HAW. REV. STAT. § 482B-1 (1993); IDAHO CODE ANN. § 48-801 (2003); 765 ILL. COMP. STAT. ANN. 1065/1 (West 2009); IND. CODE ANN. § 24-2-3-1 (LexisNexis 2006); IOWA CODE § 550.1 (2009); KAN. STAT. ANN. § 60-3320 (2005); KY. REV. STAT. ANN. § 365.880 (LexisNexis 2008); LA. REV. STAT. ANN. § 51:1431 (2003); ME. REV. STAT. tit. 10, § 1541 (2009); MD. CODE ANN., COM. LAW § 11-1201 (LexisNexis 2005); MICH. COMP. LAWS ANN. § 445.1901 (West 2002); MINN. STAT. ANN. § 325C.01 (West 2004); MISS. CODE ANN. § 75-26-1 (West 1999); MO. ANN. STAT. § 417.450 (West 2001); MONT. CODE ANN. § 30-14-401 (2009); NEB. REV. STAT. ANN. § 87-501 (LexisNexis 2007); NEV. REV. STAT. § 598A.010 (2009); N.H. REV. STAT. ANN. § 350-B:9 (LexisNexis 2008); N.M. STAT. ANN. § 57-3A-1 (1978 & Supp. 2010); N.C. GEN. STAT. ANN. § 66-153 (West 2009); N.D. CENT. CODE § 47-25.1-08 (1999); OHIO REV. CODE ANN. § 1333.61 (LexisNexis 2006 & Supp. 2010); OKLA. STAT. ANN. tit. 78, § 85 (West 2002); OR. REV. STAT. ANN. § 646.461 (West 2003); 12 PA. CONS. STAT. ANN. § 5301 (West 1999 & Supp. 2010); R.I. GEN. LAWS § 6-41-1 (2001); S.C. CODE ANN. § 39-8-10 (1976 & Supp. 2009); S.D. CODIFIED LAWS § 37-29-9 (2004); TENN. CODE ANN. § 47-25-1701 (2001); UTAH CODE ANN. § 13-24-1 (LexisNexis 2009); VT. STAT. ANN. tit. 9, § 4601 (2006); VA. CODE ANN. § 59.1-336 (2006); WASH. REV. CODE ANN. § 19.108.010 (West 1999); W. VA. CODE ANN. § 47-22-1 (LexisNexis 2006); WIS. STAT. ANN. § 134.90 (West 2009); WYO. STAT. ANN. § 40-24-101 (2009).

5. See IOWA CODE §§ 550.2–.4 (2009).

6. See, e.g., *Diversified Fastening Sys., Inc. v. Rogge*, 786 F. Supp. 1486, 1491

protection “against the disclosure or unauthorized use of the trade secret by those to whom the secret has been confided under the express or implied restriction of nondisclosure or nonuse.”⁷

The UTSA is designed to protect what the Restatement (Third) of Unfair Competition refers to as “intangible trade values.”⁸ Intangible trade values defy easy definition, but the phrase is typically interpreted to include ideas or innovations with commercial value.⁹ Intangible trade values differ from tangible assets, the dominion or control of which is commonly protected by the law of conversion.¹⁰

According to the Restatement’s comments, patent and copyright laws are the “primary” sources of protection for intangible trade values, with the laws prohibiting the misappropriation of trade secrets—both common law and statutory—providing additional protection in some instances.¹¹ All three areas of the law grant exclusive rights to the owner of intangible assets to promote and reward the creation of new ideas and technology and to prevent others from unjustly benefiting from the creator’s ingenuity and enterprise.¹² The protections afforded, however, are tempered by the recognition that granting exclusive rights to an individual or entity can “deny to the public the full benefits of valuable ideas and innovations by limiting their distribution and exploitation.”¹³

This Article discusses some of the more compelling issues arising under Iowa’s version of the UTSA. The discussion focuses on specific provisions of Iowa Code chapter 550, as well as the significant body of case law that has developed in the twenty years since the UTSA became law. Using that body of law as a platform, this Article looks at cases from other jurisdictions and commentary from legal scholars with the aim of providing additional insight into some of the more compelling trade secret issues

(N.D. Iowa 1991) (explaining both common law and statutory fiduciary duties relating to confidential business information and trade secrets (citations omitted)).

7. *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 475 (1974) (citations omitted).

8. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 38 (1995).

9. *See id.* § 38 cmt. b.

10. *E.g.*, *Kendall/Hunt Publ’g Co. v. Rowe*, 424 N.W.2d 235, 247 (Iowa 1988) (defining conversion as “the act of wrongful control or dominion over another’s personal property in denial of or inconsistent with that person’s possessory right to the property” (citations omitted)).

11. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 38 cmts. a–b, e.

12. *Id.* § 38 cmt. b.

13. *Id.*

confronting today's courts and businesspersons.

I. HOW IS A TRADE SECRET VIOLATION ESTABLISHED UNDER IOWA'S UTSA?

The UTSA prohibits the misappropriation of trade secrets.¹⁴ To establish a UTSA violation, a party must prove each of the following propositions: (1) a trade secret exists; (2) the trade secret was acquired as the result of a confidential relationship; and (3) the trade secret was used in an unauthorized manner.¹⁵ The proof necessary to establish a violation of the UTSA is similar to the proof once necessary to establish a trade secret violation under Iowa common law.¹⁶ Claims asserted under the UTSA "must be brought within three years from the date the misappropriation is discovered or should have been discovered by exercise of reasonable diligence."¹⁷

Modern trade secret law brings under one umbrella various common law tort and restitution actions that address the alleged misappropriation, infringement, or conversion of another's trade secret.¹⁸ Although trade secret law works in concert with—but does not displace or preempt—other common law claims based on similar misconduct, multiple recoveries cannot be obtained for the same injury.¹⁹ Common law claims falling into this category include actions for breach of duty, unjust enrichment, or intentional interference with existing or prospective contractual

14. See UNIF. TRADE SECRETS ACT §§ 2–3 (amended 1985), 14 U.L.A. 619, 633 (2005 & Supp. 2010).

15. *Pioneer Hi-Bred Int'l v. Holden Found. Seeds, Inc.*, 35 F.3d 1226, 1235 (8th Cir. 1994); *Walker Mfg. v. Hoffmann, Inc.*, 261 F. Supp. 2d 1054, 1079 (N.D. Iowa 2003) (citing *Lemmon v. Hendrickson*, 559 N.W.2d 278, 279 (Iowa 1997)).

16. See *Basic Chems., Inc. v. Benson*, 251 N.W.2d 220, 226 (Iowa 1977); *White Pigeon Agency, Inc. v. Madden*, No. 00-1189, 2001 WL 855366, at *6 (Iowa Ct. App. July 31, 2001) (discussing the common law elements and burden of proof for claims under the UTSA).

17. *Revere Transducers, Inc. v. Deere & Co.*, 595 N.W.2d 751, 773 (Iowa 1999) (citations omitted).

18. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 cmt. a (1995).

19. *205 Corp. v. Brandow*, 517 N.W.2d 548, 551–52 (Iowa 1994). Before adopting the UTSA, the Iowa General Assembly considered, but chose to omit, section seven of the UTSA, "which would have specifically displaced all other trade secret recoveries." *Id.* at 551. The court characterized the legislature's actions as "deliberate" and unequivocally declared, "Chapter 550 has not preempted all tort theories involving trade secrets." *Id.* at 552.

relationships.²⁰ In addition, trade secret misappropriation claims may be joined with breach of express or implied-in-fact contract claims, particularly if the claims are being asserted against a former employee, agent, or representative.²¹ The common thread running through these actions is the abuse of a confidence or trust that deprives another of proprietary information.²²

The party attempting to establish a violation of the UTSA must prove each element by a preponderance of the evidence.²³ This includes the requirement that the plaintiff identify the allegedly misappropriated trade secrets with enough particularity to permit the “defendant to delineate that which he is accused of misappropriating and a court to determine whether misappropriation has or is threatened to occur.”²⁴ The identification of “broad product and technology categories” has been found insufficient.²⁵ If the trade secrets that were allegedly taken are not stated with sufficient particularity, at least one court has observed it is “powerless to enforce a trade secret claim.”²⁶

20. *See id.* at 549–50.

21. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 40 cmt. a (1995).

22. *See id.* § 40 cmts. b–d.

23. *Lemmon v. Hendrickson*, 559 N.W.2d 278, 279 (Iowa 1997) (citing *Basic Chems., Inc. v. Benson*, 251 N.W.2d 220, 226 (Iowa 1977)).

24. *Analog Devices, Inc. v. Michalski*, 579 S.E.2d 449, 453 (N.C. Ct. App. 2003) (citations omitted); *see also* *Compuware Corp. v. Health Care Serv. Corp.*, No. 01 C 0873, 2002 WL 485710, at *7 (N.D. Ill. Apr. 1, 2002) (“[A] party alleging that its trade secrets have been misappropriated bears the burden of identifying its trade secrets with specificity.” (citing *Minn. Mining & Mfg. Co. v. Pribyl*, 259 F.3d 587, 595 n.2 (7th Cir. 2001))); *IDX Sys. Corp. v. Epic Sys. Corp.*, 165 F. Supp. 2d 812, 817 (W.D. Wis. 2001) (explaining trade secrets must be described in sufficient detail “to allow the meaningful comparison of the putative trade secret with information that is generally known and ascertainable in the relevant field or industry” (citing *Universal Analytics v. MacNeal-Schwendler Corp.*, 707 F. Supp. 1170, 1177 (C.D. Cal. 1989))).

25. *VisionAIR, Inc. v. James*, 606 S.E.2d 359, 364 (N.C. Ct. App. 2004).

26. *Guy Carpenter & Co. v. John B. Collins & Assocs., Inc.*, No. 05-1623 (JRT/FLN), 2006 WL 2502232, at *2 (D. Minn. Aug. 29, 2006); *see also* *MAI Sys. Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 522 (9th Cir. 1993) (“[A] plaintiff who seeks relief for misappropriation of trade secrets must identify the trade secrets and carry the burden of showing that they exist.” (citations omitted)); *Sun Media Sys., Inc. v. KD SM, LLC*, 564 F. Supp. 2d 946, 965 (S.D. Iowa 2005) (noting the plaintiff “cannot rely on generic categories or assertions, but rather must assert *specific* allegations that it possessed information that meets the definition of trade secret under IUTSA, and must proffer evidence that Defendants actually received the trade secret and improperly used it”).

II. WHAT IS A TRADE SECRET?

The initial point of inquiry in most trade secret cases is whether the information that was allegedly misappropriated constitutes a trade secret. That issue is typically analyzed first because if the misappropriated information is a trade secret, a viable trade secret claim may exist depending upon the resolution of other issues. If, on the other hand, the misappropriated information is not a trade secret, a valid trade secret claim cannot be established although other causes of action may apply. The information constituting a trade secret typically turns upon the facts of a given case, which, in many instances, are disputed.

As adopted in Iowa, the UTSA broadly defines a trade secret as

[I]nformation, including but not limited to a formula, pattern, compilation, program, device, method, technique, or process that . . . [d]erives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by a person able to obtain economic value from its disclosure or use . . . [and] [i]s the subject of efforts that are reasonable under the circumstances to maintain its secrecy.²⁷

The Iowa Supreme Court has stated that “[t]here is virtually no category of information that cannot, as long as the information is protected from disclosure to the public, constitute a trade secret.”²⁸ Despite that broad pronouncement, the specific categories of potential trade secret information typically “include customer, financial, and manufacturing process information, as well as the composition of products.”²⁹ Furthermore, other types of business information may also qualify as trade secrets, including the “maintenance of data on customer lists and needs, source of supplies, confidential costs, price data and figures,”³⁰ even though none of those information types are specifically listed within the statutory definition.³¹

27. IOWA CODE § 550.2(4) (2009).

28. *US W. Commc'ns, Inc. v. Office of Consumer Advocate*, 498 N.W.2d 711, 714 (Iowa 1993) (quoting Thomas J. Collin, *Determining Whether Information Is a Trade Secret Under Ohio Law*, 19 U. TOL. L. REV. 543, 545 (1988)).

29. *Bus. Designs, Inc. v. Midnational Graphics, L.L.C.*, No. 01-1087, 2002 WL 987971, at *2 (Iowa Ct. App. May 15, 2002) (citing *Revere Transducers, Inc. v. Deere & Co.*, 595 N.W.2d 751, 776 (Iowa 1999)).

30. *Revere*, 595 N.W.2d at 776.

31. *See* IOWA CODE § 550.2(4) (2009).

Whether confidential information rises to the level of a trade secret is a mixed question of fact and law.³² The legal aspect of the question pertains to whether the information is embodied in the first part of Iowa's UTSA definition of a trade secret—whether the information is “a formula, pattern, compilation, program, device, method, technique, or process.”³³ The factual aspect of the question pertains to the remaining portion of the definition—whether the requirements of subsections (a) and (b) to section 550.2(4) are met.³⁴ Given the Iowa Supreme Court's pronouncement “[t]here is virtually no category of information” that cannot, at least in theory, qualify as a trade secret, most trade secret cases turn upon factual, as opposed to legal, issues.³⁵

The factual criteria considered by courts in determining what information constitutes a trade secret will, of course, vary from case to case. However, courts have centered their inquiry upon the following factors:

(1) [T]he extent to which the information is known outside of [the owner's] business; (2) the extent to which [the information] is known by employees and others involved in [the owner's] business; (3) the extent of measures taken by [the owner] to guard the secrecy of the information; (4) the value of the information to [the owner] and to [the owner's] competitors; (5) the amount of effort or money expended by [the owner] in developing the information; [and] (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.³⁶

These factors are consistent with the UTSA's definition of trade secret, and the factors properly focus the court's attention on the value and

32. *Econ. Roofing & Insulating Co. v. Zumaris*, 538 N.W.2d 641, 648 (Iowa 1995).

33. *Id.* (quoting IOWA CODE § 550.2(4) (1991)).

34. *Id.* at 648–49 (citing IOWA CODE § 550.2(4) (1991)).

35. *Cf. Cent. States Indus. Supply, Inc. v. McCullough*, 279 F. Supp. 2d 1005, 1038 (N.D. Iowa 2003) (quoting *US W. Commc'ns, Inc. v. Office of Consumer Advocate*, 498 N.W.2d 711, 714 (Iowa 1993)) (explaining on summary judgment the court identifies genuine issues of material fact that become issues for the jury).

36. RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939); *accord* *Learning Curve Toys, Inc. v. PlayWood Toys, Inc.*, 342 F.3d 714, 722 (7th Cir. 2003); *N. Atl. Instruments, Inc. v. Haber*, 188 F.3d 38, 44 (2d Cir. 1999); *Baxter Int'l, Inc. v. Morris*, 976 F.2d 1189, 1193 (8th Cir. 1992); *Am. Sci. & Eng'g, Inc. v. Kelly*, 69 F. Supp. 2d 227, 238 (D. Mass. 1999); *Cemen Tech, Inc. v. Three D Indus.*, 753 N.W.2d 1, 7 (Iowa 2008); *Kendall/Hunt Publ'g Co. v. Rowe*, 424 N.W.2d 235, 246 (Iowa 1988).

secrecy of the information for which trade secret status is sought.

Although the UTSA defines what constitutes a trade secret in relatively general terms, the definition is case specific and not easily applied to broad categories of information. For example, the prices a company charges for its products or services are generally considered to be proprietary in nature, and pricing information certainly satisfies the legal test for a trade secret.³⁷ However, whether specific pricing information constitutes a trade secret typically turns upon whether the pricing information derives independent economic value because it is secret and whether the company has taken reasonable measures to keep its prices confidential.³⁸ Issues that can arise regarding those two points include the following:

- Does the pricing information have independent economic value because the company's competitors do not generally know the information? Or alternatively, does every company in the relevant marketplace know what prices its competitors charge?
- What steps did the company take to protect the purported secrecy of its pricing information?
- How does the company handle the information internally? Does it disclose the information only to those employees or representatives having a need to know the information?
- Does the company require actual or prospective customers to sign nondisclosure agreements regarding the prices it offers those entities? Does it even mark its pricing proposals as being confidential?
- Do the company's customers routinely share the pricing information with the company's competitors? Does the company have any of its competitor's pricing proposals?

The alleged misappropriation of computer software raises many interesting trade secret issues, including whether the software or its components meet the definition of a protected trade secret. Source code that has not been publicly disclosed is generally considered trade secret

37. *Synergetics, Inc. v. Hurst*, 477 F.3d 949, 957–58 (8th Cir. 2007); *EFCO Corp. v. Symons Corp.*, 219 F.3d 734, 741 (8th Cir. 2000).

38. *See EFCO Corp.*, 219 F.3d at 741.

information.³⁹ However, trade secret protection is not necessarily limited to source code, and at least one court has stated “the overall *design* of a software program may be protectable as a trade secret, even if the individual *components* of that program are common knowledge in the programming industry.”⁴⁰ This recognition is based on the more general proposition that “[a] trade secret can exist in a combination of characteristics and components, each of which, by itself, is in the public domain, but the unified process design and operation of which in unique combination affords a competitive advantage and is a protectable trade secret.”⁴¹

Determining whether certain information is a trade secret often requires courts to distinguish between information that is proprietary to a specific company and information that is generally known within a particular industry or field. This issue commonly arises in cases when an employee who is not subject to a noncompete agreement leaves his employer and begins working in the same or similar capacity with a competitor. In those situations, it is generally recognized the departing employee can use the general knowledge, skill, and expertise he possesses, even if all or some of that knowledge, skill, and expertise was obtained during, or as a result of, the departing employee’s prior employment.⁴² However, the employee cannot disclose or use his former employer’s trade secrets. Distinguishing between those two categories of information can be difficult—particularly if the departing employee held a high-level management position with his former employer and was exposed to a myriad of confidential information.

In these types of departing employee cases, courts must differentiate knowledge, skill, and know-how that is general—in the sense it can be

39. *TouchPoint Solutions, Inc. v. Eastman Kodak Co.*, 345 F. Supp. 2d 23, 28 (D. Mass. 2004) (citing *Harbor Software, Inc. v. Applied Sys., Inc.*, 887 F. Supp. 86, 90 (S.D.N.Y. 1995)).

40. *Harbor Software, Inc.*, 887 F. Supp. at 90 (citations omitted).

41. *Computer Care v. Serv. Sys. Enters., Inc.*, 982 F.2d 1063, 1074 (7th Cir. 1992) (quoting *SmokEnders, Inc. v. Smoke No More, Inc.*, 184 U.S.P.Q. (BNA) 309, 317 (S.D. Fla. 1974)).

42. *See Hogan Sys., Inc. v. Cybresource Int’l, Inc.*, 158 F.3d 319, 324 (5th Cir. 1998) (holding general knowledge, skill, and experience gained by employees during employment with prior employer did not constitute a trade secret); *FMC Corp. v. Cyprus Foote Mineral Co.*, 899 F. Supp. 1477, 1483 (W.D.N.C. 1995) (noting a former employee with “a great deal of general skill and knowledge as an engineer who ha[d] worked for 14 years in the area of lithium production” was “free to sell those skills in the marketplace”).

applied in varying situations and within multiple contexts—from secret information that is specific to the former employer’s particular techniques, processes, procedures, customers, suppliers, finances, or pricing methods.⁴³ Arguably, only information the employer has taken reasonable steps to keep secret, and is specific to the employer’s operations, warrants trade secret protection. In contrast, prohibiting a departing employee from using information and know-how that has generalized application and is not treated as confidential unduly hamstrings his employment options and unnecessarily restricts legitimate competition.⁴⁴

III. WHAT DOES IT MEAN TO DERIVE ECONOMIC VALUE FROM NOT BEING KNOWN OR READILY ASCERTAINABLE THROUGH PROPER MEANS?

Many of the factual issues that arise in trade secret cases pertain to the first prong of the UTSA’s trade secret definition. That prong, as noted above, requires trade secret information to derive independent economic value from not being known, or readily ascertainable through proper means, by a person to whom the information has potential value.⁴⁵ Iowa courts have broadly interpreted this prong to include any information that gives its owner a “competitive edge or advantage.”⁴⁶ The requisite competitive edge or advantage must, however, arise because the information is not generally known and cannot easily be replicated.⁴⁷

Information that can, at least in theory, be otherwise ascertained through proper means does not necessarily defeat a trade secret claim if

43. See *Cemen Tech, Inc. v. Three D Indus.*, 753 N.W.2d 1, 8 (Iowa 2008). The court found genuine issues of fact existed regarding whether information former employees of Cemen Tech obtained regarding the company’s cement volumetric mixer, the mixer’s component parts, and the company’s manufacturing processes, suppliers, and customers constituted protected trade secrets. *Id.* at 8–11. The court found issues of fact existed regarding whether the information had “economic value” because company representatives “identified numerous processes and design features developed by CTI that were unique, features that CTI had sought to protect by its confidentiality agreements and which it claimed trade secrets.” *Id.* at 8.

44. See *FMC Corp.*, 899 F. Supp. at 1483 (holding the general knowledge and skill an employee acquired by working fourteen years in the area of lithium production was not a trade secret because that knowledge and skill was “not specific to the techniques and processes utilized by FMC”).

45. See IOWA CODE § 550.2(4) (2009).

46. *Olson v. Nieman’s Ltd.*, 579 N.W.2d 299, 314 (Iowa 1998) (quoting *US W. Commc’ns, Inc. v. Office of Consumer Advocate*, 498 N.W.2d 711, 714 (Iowa 1993)).

47. *Id.*

acquiring the information through proper means “would be difficult, costly, or time-consuming.”⁴⁸ For example, if a company’s customers are widely known within a particular industry, and the names, addresses, and phone numbers of those customers can easily be obtained by using a phone book, the Internet, or some other outside source in the public domain, a list containing customer contact information may not constitute a trade secret.⁴⁹ If, in contrast, the company’s customers are not widely known, or if the customer list contains contact information of key employees whose identities took significant time and effort to obtain, the list will, in all likelihood, be considered a trade secret if the other conditions necessary to establish the existence of a trade secret are met.⁵⁰ The determinative issue in both examples is whether the list can be replicated through proper means with little effort. If it cannot, possessing the list provides its owner with a competitive advantage. As one commentator observed: “[I]n business most matters are considered confidential; however, only secrets affording a demonstrable competitive advantage may be properly

48. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. f (1995).

49. *E.g.*, *CDI Energy Servs., Inc. v. W. River Pumps, Inc.*, 567 F.3d 398, 402 (8th Cir. 2009) (holding a list of prospective customers was not a trade secret where the list consisted of “a small collection of easily identifiable, locally operating oilfield companies, [and] information about these companies would be easily obtainable, if not already known, by relevant actors in the local oilfield service and equipment industry”); *Heartland Home Fin., Inc. v. Allied Home Mortg. Capital Corp.*, 258 F. App’x 860, 862 (6th Cir. 2008) (finding lead information was not a trade secret where the information was “merely ‘raw data’ used to garner mortgage sales” that was “openly available on the market at minimal cost”).

50. *See, e.g.*, *Hertz v. Luzenac Grp.*, 576 F.3d 1103, 1114 (10th Cir. 2009) (holding, under Colorado’s UTSA, “[a] customer list can be a trade secret when it is the end result of a long process of culling the relevant information from lengthy and diverse sources, even if the original sources are publicly available” (citations omitted)); *Conseco Fin. Servicing Corp. v. N. Am. Mortg. Co.*, 381 F.3d 811, 819 (8th Cir. 2004) (determining lead sheets and other information contained in Conseco’s customer files were trade secrets under the Missouri UTSA because the information was compiled by a “specialized—and apparently quite effective—computer program that was uniquely Conseco’s”); *Bro-Tech Corp. v. Thermax, Inc.*, 651 F. Supp. 2d 378, 389, 409 (E.D. Pa. 2009) (holding “[a] compilation of customer data may qualify as a trade secret if it is not readily obtainable from another source and was generated in such a fashion that it constitutes intellectual property of the owner,” and stating genuine issues of fact existed regarding whether certain sales and customer information qualified as a trade secret (citations omitted)); *Am. Family Mut. Ins. Co. v. Hollander*, No. C08-1039, 2009 WL 535990, at *14 (N.D. Iowa Mar. 3, 2009) (concluding “it is likely” the plaintiff insurance company would be able to prove at trial “the names and addresses of its customers constituted a ‘trade secret’ under either Iowa or Wisconsin law”).

considered trade secrets.”⁵¹

Whether information is readily ascertainable through proper means is a different question than whether the information was, in fact, obtained in that manner. That a product, device, software program, or similar item can, in theory, be reverse-engineered with little effort is relevant to determining whether the item is “readily ascertainable by proper means” and therefore truly secret.⁵² If the item can be reverse-engineered with ease, the item is readily ascertainable and arguably not a trade secret. Moreover, this argument—that the item is readily ascertainable because it is subject to reverse engineering—can be made even if the item was developed through the acquisition of another’s know-how and not actually reverse-engineered.⁵³

That a product, device, list, or item was acquired through independent means—actually reverse-engineered—is a defense to a misappropriation of trade secret claim even if the product, device, list, or other item meets the definition of a trade secret.⁵⁴ Reverse engineering exists as a complete defense because trade secret law prohibits only the “*wrongful* acquisition, use, or disclosure of the trade secret.”⁵⁵ Unlike patent law, trade secret law does not grant the trade secret owner “an exclusive right to possession or use of the secret information,” and it does not provide the owner with a “claim against another who independently discovers the secret.”⁵⁶ As a result, a company can reverse-engineer a competitor’s products, or some aspect of a product, provided it does so by

51. 1 ROGER M. MILGRIM & ERIC E. BENSON, MILGRIM ON TRADE SECRETS § 1.03 (2010) (footnotes omitted).

52. See, e.g., *Revere Transducers, Inc. v. Deere & Co.*, 595 N.W.2d 751, 775 (Iowa 1999). Reverse engineering is defined as “the process by which a completed process is systematically broken down into its component parts to discover the properties of the product with the goal of gaining the expertise to reproduce the product.” *Id.* at 775 n.8 (quoting *Christianson v. Colt Indus. Operating Corp.*, 870 F.2d 1292, 1295 n.4 (7th Cir. 1989)).

53. E.g., *Walker Mfg. v. Hoffmann, Inc.*, 261 F. Supp. 2d 1054, 1081 (N.D. Iowa 2003) (noting “the possibility that certain matters can be discovered by ‘reverse engineering’ is relevant to whether or not they are protectable trade secrets” and can be raised even if the defendant “does not assert, as a defense to a claim of misappropriation of trade secrets, that it in fact obtained those matters by reverse engineering”).

54. See *id.*

55. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 43 cmt. a (1995) (emphasis added).

56. *Id.* § 43 cmts. a–b.

deconstructing and rebuilding the product or through some other proper means.⁵⁷ Stated conversely, “[t]he owner of a trade secret is not entitled to prevent others from using public information to replicate his product, nor may the owner prevent others from making similar products which are not derived from the trade secret.”⁵⁸

Iowa courts have recognized that even if a trade secret contained within a product can be discovered through reverse engineering, the secret may still have economic value and qualify as a trade secret provided the product has not been offered for sale or otherwise disclosed to the public. The Iowa Supreme Court first applied this rule in *Olson v. Nieman's, Ltd.*⁵⁹ In that case, the court concluded a device that activated flashing lights in the event of a trailer breakaway had potential economic value even though the defendant argued the device was essentially worthless because any engineer could have purchased the product and reverse-engineered the device once it was introduced into the marketplace.⁶⁰ The Iowa Supreme Court found the device retained potential economic value because Olson, the inventor of the device, had options other than selling the device in the marketplace and thus destroying its value.⁶¹ According to the court, Olson could have sold his idea to a manufacturer or patented the idea had Nieman, the defendant, not misappropriated the idea and disclosed it to the public.⁶²

There is some tension between the Iowa Supreme Court's decision in *Olson* and its later decision in *Revere Transducers, Inc. v. Deere & Co.*⁶³ In *Revere*, the court approved a jury instruction that listed the factors the jury could take into account when determining whether certain aspects of a draft sensor device were trade secrets. The instruction told the jury it could consider, among other things, “[t]he ease or difficulty with which the information could be properly acquired or duplicated by others.”⁶⁴ The court held the instruction was proper and further concluded the trial court correctly declined to instruct the jury that “[t]he fact that one could have obtained a trade secret lawfully is not a defense if one does not actually use

57. *Id.*

58. *Am. Can Co. v. Mansukhani*, 742 F.2d 314, 329 (7th Cir. 1984) (citations omitted).

59. *Olson v. Nieman's, Ltd.*, 579 N.W.2d 299, 314 (Iowa 1998).

60. *Id.*

61. *Id.*

62. *Id.*

63. *Revere Transducers, Inc. v. Deere & Co.*, 595 N.W.2d 751 (Iowa 1999).

64. *Id.* at 775.

proper means to acquire the information.”⁶⁵ The *Revere* Court’s approval of the instruction permitting the jury to consider, at the outset, the effort it would take to discover a trade secret through reverse engineering is inconsistent with *Olson* to a certain extent. As previously discussed, the court in *Olson* held that idea or concept, even if ascertainable through reverse engineering, still has economic value and may be a trade secret if it remained secret and had not been released in the marketplace.⁶⁶

This apparent inconsistency was addressed in *Walker Manufacturing, Inc. v. Hoffmann, Inc.*, a case involving the alleged misappropriation of trade secrets pertaining to the design and sale of self-propelled crop sprayers.⁶⁷ In that case, Hoffman, the defendant, denied Walker Manufacturing’s drawings were used significantly in developing a competing crop sprayer.⁶⁸ Hoffman also argued, in the alternative, the drawings were not protected trade secrets anyway.⁶⁹ Hoffman asserted Walker Manufacturing had placed the product on the market, thus any secrets contained in the drawings were lost at that point.⁷⁰ Hoffman further argued the secrets were discoverable through reverse engineering with little difficulty.⁷¹

Similar to the inventors in *Olson* and *Revere*, Walker Manufacturing maintained whether the trade secrets contained within its drawings could be discovered through reverse engineering was largely irrelevant because Hoffman did not contend it actually reverse-engineered Walker Manufacturing’s crop sprayers.⁷² In addition, Walker Manufacturing argued, consistent with the Iowa Supreme Court’s holding in *Olson*, “that, so long as it derived some value from keeping the information secret and made attempts to keep it secret, the information is considered a trade secret under Iowa law.”⁷³

The *Walker Manufacturing* Court reconciled the tension between the Iowa Supreme Court’s *Olson* and *Revere* decisions by concluding whether

65. *Id.*

66. *Olson*, 579 N.W.2d at 314.

67. *Walker Mfg., Inc. v. Hoffmann, Inc.*, 261 F. Supp. 2d 1054 (N.D. Iowa 2003).

68. *Id.* at 1060.

69. *Id.* at 1079.

70. *Id.* at 1078.

71. *Id.*

72. *Id.* at 1079.

73. *Id.*

an idea or concept can be discovered through reverse engineering is relevant to determining whether the device or idea meets the definition of trade secret only if the idea or concept “has been publicly disclosed, for example, by public sales of the device.”⁷⁴ If, on the other hand, “the inventor has taken reasonable steps to maintain the secrecy of the [idea or concept]” and has not offered the device for public sale, then whether the idea or concept is readily ascertainable through reverse engineering is irrelevant when determining whether the idea or concept is a trade secret.⁷⁵

The *Walker Manufacturing* Court’s synthesis of *Olson* and *Revere* is based on a fair reading of each case and properly reconciles the competing interests involved when a company acquires information or know-how that has not been disclosed through public sale or is otherwise not part of the public domain. For those instances, the information may be readily ascertainable through reverse engineering, but that theoretical possibility is not material because the information or know-how remains secret and cannot be readily ascertained through “proper means.” In other words, a competitor would have to resort to theft or other acts of industrial espionage to acquire the secret and cannot discover the secret through the deconstruction and rebuilding of a competing product.

Reverse engineering was also discussed in the Iowa Supreme Court’s more recent trade secret decision, *Cemen Tech, Inc. v. Three D Industries*.⁷⁶ That decision involved, among other claims, the alleged misappropriation of trade secret information by a group of former employees of Cemen Tech, Inc. (CTI).⁷⁷ The former CTI employees went to work for the defendant, Three D Industries (Three D), and within six months, Three D developed mobile, volumetric concrete mixers that competed directly with CTI’s products.⁷⁸ Three D asserted, in response to CTI’s trade secret claims, any information and know-how its owners allegedly misappropriated did not constitute protected trade secrets because, among other things, the information was readily ascertained through reverse engineering.⁷⁹ The trial court agreed with Three D and granted summary judgment in its favor.⁸⁰

74. *Id.* at 1082 (citing *Revere Transducers, Inc. v. Deere & Co.*, 595 N.W.2d 751, 775–76 (Iowa 1999)).

75. *Id.* (citing *Olson v. Nieman’s Ltd.*, 579 N.W.2d 299, 314 (Iowa 1998)).

76. *Cemen Tech, Inc. v. Three D Indus.*, 753 N.W.2d 1 (Iowa 2008).

77. *Id.* at 6.

78. *Id.* at 4.

79. *Id.* at 9.

80. *Id.* at 8–10.

On appeal, CTI conceded that if given sufficient time, Three D could have manufactured a machine similar to CTI's mixer; however, CTI pointed to the testimony of its expert witness, a mechanical engineer, who opined it would have taken "even a trained and experienced engineer" far longer than the six months it took Three D's owners to create a competing product.⁸¹ CTI argued the testimony of its expert witness showed an issue of fact regarding whether the information Three D purportedly used was readily ascertainable.⁸² The Iowa Supreme Court agreed with CTI, observing, "[the expert's] report [was] strong evidence that, though CTI's machine and component parts could be reverse engineered, the difficulty in doing so may not defeat CTI's trade-secret claim."⁸³ In addition, the court found the information, even if it could be discovered through reverse engineering, had economic value as "a fact finder could reasonably conclude that the delay in production of the machine would give CTI a temporal advantage."⁸⁴ Moreover, the temporal advantage Three D gained, no matter how fleeting, was potentially actionable "because neither Iowa Code section 550.2(4) nor section 1(4) of the Uniform Trade Secrets Act 'include[s] any requirement relating to the duration of the information's economic value.'"⁸⁵

The *Cemen Tech* decision is important to Iowa trade secret law for at least two reasons. First, the decision establishes confidential information can qualify as a trade secret even if the information could, theoretically, be obtained through reverse engineering, assuming it would require significant time and resources to obtain the confidential information through that process.⁸⁶ Second, and perhaps more importantly, the decision demonstrates confidential information has economic value if the information would give the misappropriating party a competitive edge or what the court referred to as a "temporal advantage."⁸⁷ This is true even if the competitive edge is slight or the temporal advantage brief.⁸⁸ As the court observed, "Presumably, the extent of this temporal advantage would

81. *Id.*

82. *Id.*

83. *Id.* at 10.

84. *Id.*

85. *Id.* (quoting RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. d (1995)).

86. *Id.*

87. *Id.*

88. *Id.*

be reflected in any damage award.”⁸⁹

IV. ARE CUSTOMER LISTS TRADE SECRETS?

One of the common misperceptions about trade secret law is customer lists and other information pertaining to the entities with whom a company does business are, almost by definition, trade secrets protected from unauthorized disclosure or use. Like other information, customer lists and related information must meet the statutory criteria to be protected as a trade secret under the UTSA.⁹⁰ In other words, the party seeking protection must show, among other things, it developed the list or obtained the information through substantial effort, it took reasonable efforts to protect the information's secrecy, and the information could not be obtained with relative ease from other sources.⁹¹

The Iowa Supreme Court first addressed whether customer lists and other customer information could be protected trade secrets in *Basic Chemicals, Inc. v. Benson*.⁹² That case involved a bitter dispute between Basic Chemicals, a company that manufactured sanitation products and supplies, and Richard Benson, the company's former president and general manager.⁹³ Benson left Basic Chemicals to join a competitor and took with him documents containing confidential information he developed or acquired during his employment with Basic Chemicals.⁹⁴ The documents Benson purloined included, among other things, detailed customer lists containing the names and addresses of all of Basic Chemicals's customers.⁹⁵ He also took with him other sundry customer information such as “the proper time to call on specific customers; the names of key employees of customers; the names of spouses and children of individual customers as well as their birthdays, together with particular likes and dislikes of specific customers.”⁹⁶

Relying on the definition of trade secret that was, at that time, stated in section 757 of the Restatement of Torts—the UTSA had yet to be

89. *Id.*

90. UNIF. TRADE SECRETS ACT § 1(4) (amended 1985), 14 U.L.A. 538 (2005 & Supp. 2010).

91. *See id.*

92. *Basic Chems., Inc. v. Benson*, 251 N.W.2d 220 (Iowa 1977).

93. *Id.* at 223.

94. *Id.*

95. *Id.* at 228.

96. *Id.*

enacted—the court concluded the information contained in the stolen customer books were trade secrets and the books belonged to Basic Chemicals, not Benson.⁹⁷ In making that determination, the court observed Basic Chemicals “had a policy of maintaining the information in the customer books secret” and “[t]here was only one set and Benson was the only person given unlimited access to those books.”⁹⁸ The court further found the nature and type of information contained in the books confirmed the books were compiled through substantial effort, and the customer books, combined with formula books, contained unique customer data that gave Basic Chemicals a competitive advantage.⁹⁹ As the court observed, the books contained “information [the company] learned that would be useful in developing and maintaining a successful relationship with a customer.”¹⁰⁰

Lawyers have a tendency to mistakenly cite *Basic Chemicals* for the general proposition that all information pertaining to a business’s customers should be regarded as a trade secret. Such a broad interpretation overlooks the fact-intensive inquiry that must be undertaken in any trade secret case and ignores the nature and extent of the customer information at issue in that decision. As a general matter, contact lists and similar records merely identifying the names and addresses of a company’s customers and containing other information that is generally known within a given industry or is readily ascertainable from published sources are not considered trade secrets.¹⁰¹ An exception to this general rule exists if a company “‘expends a great deal of time, effort and expense’” compiling generally known or readily ascertainable information and then takes reasonable efforts to keep the compilation secret.¹⁰² Thus, even if gathered

97. *Id.* at 230.

98. *Id.* at 229.

99. *Id.*

100. *Id.* at 228. Further, in *White Pigeon Agency, Inc. v. Madden*, the Iowa Court of Appeals held a list maintained by an insurance company containing the names of its customers, as well as the insurance policies it purchased and the renewal dates for those policies, was a trade secret within the meaning of IOWA CODE § 550.2 (2001). *White Pigeon Agency, Inc. v. Madden*, No. 00–1189, 2001 WL 855366, at *7 (Iowa Ct. App. July 31, 2001).

101. See, e.g., *Vigoro Indus., Inc. v. Crisp*, 82 F.3d 785, 789–90 (8th Cir. 1996) (holding, because the customers were from a small geographic area, records identifying two hundred customers and showing each customer’s planting history, prior purchases, and credit history were easily discoverable and therefore not trade secrets).

102. *Fireworks Spectacular, Inc. v. Premier Pyrotechnics, Inc.*, 147 F. Supp. 2d 1057, 1066 (D. Kan. 2001) (quoting *Robert B. Vance & Assocs., Inc. v. Baronet Corp.*, 487 F. Supp. 790, 799 (N.D. Ga. 1979)).

information “is ultimately ascertainable from public sources,” the compilation potentially qualifies as a trade secret if “it is not *readily* ascertainable from public sources.”¹⁰³

An issue commonly arising in trade secret cases involving the alleged misappropriation of customer lists is whether a departing employee can use or disclose customer information the employee obtained during a time of former employment if the employee later recalls the information, but has not taken any records from the former employer. The Iowa Supreme Court first addressed that issue in *Lemmon v. Hendrickson* and concluded a former employee was entitled to use general business information he or she obtained, as well as “*the names of the customers retained in his memory*, if not acquired in violation of his duty as an agent.”¹⁰⁴

The *Lemmon* case involved a dispute between a pest control company and one of its former technicians.¹⁰⁵ The pest control company alleged the technician used its customer list to steal seven customers.¹⁰⁶ The alleged misappropriation happened two years after the technician left the company and after he unsuccessfully pursued a different business venture.¹⁰⁷ The technician defended himself by denying he retained any customer lists after he left the pest control company.¹⁰⁸ He simply recalled the names of former customers and contacted those customers “from that recollection.”¹⁰⁹ While acknowledging “a customer list can be a protected trade secret under certain conditions,” the court in *Lemmon* concluded the technician’s use of customer information he acquired during his prior employment did not violate Iowa common law.¹¹⁰ The court’s decision was

103. *Id.* (emphasis added).

104. *Lemmon v. Hendrickson*, 559 N.W.2d 278, 280–81 (Iowa 1997) (quoting RESTATEMENT (SECOND) OF AGENCY § 396 (1958)). *But see* Cemen Tech, Inc. v. Three D. Indus., 753 N.W.2d 1, 7 (Iowa 2008) (“A trade secret need not be in writing; any secret acquired through an employee’s job may be the subject of trade-secret protection.” (citing *Sperry Rand Corp. v. Rothlein*, 241 F. Supp. 549, 563 (D. Conn. 1964))).

105. *Lemmon*, 559 N.W.2d at 279.

106. *Id.*

107. *Id.*

108. *Id.* at 280.

109. *Id.*

110. *Id.* at 280–81 (citing *Basic Chems., Inc. v. Benson*, 251 N.W.2d 220, 230 (Iowa 1977)); *see also* *Educ. Tech., Ltd. v. Meinhard*, No. 99-0689, 2001 WL 488088, at *5 (Iowa Ct. App. May 9, 2001) (holding former employees were entitled to take with them “their personal effects, their memories, and a Rolodex containing the names of distributors and suppliers”).

based in part upon the Restatement (Second) of Agency, which, at that time, allowed a departing employee “to use general information concerning the method of business of the principal *and the names of the customers retained in his memory*, if not acquired in violation of his duty as an agent.”¹¹¹

A slightly different result was reached in *Merrill Lynch v. Evans*, a case in which three former Merrill Lynch stockbrokers joined Dean Witter, a competing brokerage.¹¹² Merrill Lynch claimed the brokers were using confidential customer information to transfer or “flip” accounts to their new employer in violation of a previously issued injunction.¹¹³ The brokers denied using Merrill Lynch’s records.¹¹⁴ Instead, they claimed the customers they were able to flip either contacted them directly or were contacted through the use of a new list the brokers constructed “utilizing [their] own memor[ies], commercially available computer software, and the Internet.”¹¹⁵

The court in *Evans* concluded the three brokers did not violate the injunction by flipping the accounts of customers who independently contacted them.¹¹⁶ With respect to those customers, the court found “Merrill Lynch customers should continue to enjoy their rights as consumers to pick and choose their money managers.”¹¹⁷ The court, however, reached a different result regarding the newly constructed customer lists.¹¹⁸ With respect to those lists, the court determined the brokers’ actions violated the injunction because the term “customer lists,” both as contained in the previously issued injunction and as defined in the various agreements the brokers signed during their employment with Merrill Lynch, included “not only tangible documents and records,” but also “the information contained therein,” which the brokers clearly used.¹¹⁹ Based on that finding, the court expanded its prior injunction to prohibit the brokers from not only using customer information as so defined, but

111. See *Lemmon*, 559 N.W.2d at 280–81 (quoting RESTATEMENT (SECOND) OF AGENCY § 396 (1958)).

112. *Merrill Lynch, Pierce, Fenner & Smith Inc. v. Evans*, No. 3-00-CV-90220, 2000 WL 33363253, at *1 (S.D. Iowa Dec. 22, 2000).

113. *Id.*

114. *Id.*

115. *Id.*

116. *Id.*

117. *Id.*

118. *Id.*

119. *Id.* at *2.

also from creating any additional “lists for the purpose of contacting former Merrill Lynch customers and facilitating account transfers to Dean Witter.”¹²⁰

Even though the court in *Evans* did not specifically find the customer information contained in the newly created lists was a trade secret, there is discernable tension between that court’s conclusion and the Restatement approach adopted by the Iowa Supreme Court in *Lemmon*. Information stored in a person’s mind was fair game, according to the court in *Lemmon*,¹²¹ while the same information was the subject of an expanded injunction in *Evans*.¹²² The result in *Evans*, however, is consistent with the decisions of other courts and the views of many commentators who have criticized the Restatement approach, often referred to as the “memory rule,” because the approach places too much emphasis on the medium in which the information is stored—memory versus some “tangible form”—and, in so doing, ignores the nature and character of the information that is taken, as well as the means through which the information is gained.¹²³

The result in *Evans* is also consistent with the Iowa Supreme Court’s decision in *Cemen Tech, Inc. v. Three D Industries*, in which the court generally recognized trade secrets “need not be in writing” and “any secret acquired through an employee’s job may be the subject of trade-secret protection.”¹²⁴ Even though *Cemen Tech* involved the alleged misappropriation of confidential information regarding the design and sale of mobile, volumetric concrete mixers, there is no reason to believe the court will, in the future, apply different legal principles to cases involving the alleged misappropriation of confidential customer information.

V. WHAT EFFORTS MUST BE MADE TO KEEP CONFIDENTIAL INFORMATION SECRET?

To be a trade secret, information must be subject to “reasonable efforts” to keep the information secret.¹²⁵ What constitutes reasonable

120. *Id.* at *3.

121. *See* *Lemmon v. Hendrickson*, 559 N.W.2d 278, 280–81 (Iowa 1997).

122. *Evans*, 2000 WL 33363253, at *3.

123. *See* *Ed Nowogroski Ins., Inc. v. Rucker*, 971 P.2d 936, 947 (Wash. 1999) (citing 2 RUDOLF CALLMANN, *THE LAW OF UNFAIR COMPETITION, TRADEMARKS AND MONOPOLIES* § 14.31 (4th ed. & Supp. 1996)).

124. *Cemen Tech, Inc. v. Three D Indus.*, 753 N.W.2d 1, 7 (Iowa 2008) (citing *Sperry Rand Corp. v. Rothlein*, 241 F. Supp. 549, 563 (D. Conn. 1964)).

125. *See* *205 Corp. v. Brandow*, 517 N.W.2d 548, 550 (Iowa 1994) (citing IOWA CODE § 550.2(4) (1991)).

efforts depends upon the circumstances of each case, including the special needs of the business claiming a misappropriation of a trade secret.¹²⁶

The requirement that individuals or businesses take reasonable efforts to protect the confidentiality of trade secret information

lies in the fact that if the plaintiff has allowed his trade secret to fall into the public domain, he would enjoy a windfall if permitted to recover damages merely because the defendant took the secret from him, rather than from the public domain as it could have done with impunity.¹²⁷

Taking reasonable efforts to keep the information secret also puts “prospective infringers on notice about the existence of a right and serve[s] as evidence of the fact that the secret is worth protecting legally.”¹²⁸

Trade secrets owned by companies often must be disclosed internally—and sometimes externally—for the trade secret to have any value to the company.¹²⁹ Appreciating that reality, Iowa courts have recognized the following measures companies can take to protect the confidential nature of their trade secrets:

1) [R]equiring employees to sign confidentiality agreements or otherwise advising them of the confidential nature of the process; 2) posting of warning or cautionary signs, or placing legends on documents; 3) taking precautions regarding visitors, by requiring them to sign confidentiality agreements, having them sign in, and shielding the process from their view; 4) segregating information, so that no one person or written source discloses the entire manufacturing process; 5) using unnamed or code-named ingredients; and 6) keeping secret documents under lock.¹³⁰

126. *Id.* at 551.

127. *Bus. Designs, Inc. v. Midnational Graphics, L.L.C.*, No. 01-1087, 2002 WL 987971, at *4-5 (Iowa Ct. App. May 15, 2002) (Hecht, J., dissenting) (quoting *Rockwell Graphic Sys., Inc. v. DEV Indus., Inc.*, 925 F.2d 174, 179 (7th Cir. 1991)).

128. *Id.* at *5 (citing ROBERT P. MERGES ET AL., *INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGY AGE* 59 (5th ed. 2009)).

129. *See id.* at *3-4 (majority opinion).

130. *See id.* at *5 (Hecht, J., dissenting) (citations omitted). The Restatement (Third) of Unfair Competition provides similar examples and states, in relevant part, “Precautions to maintain secrecy may take many forms, including physical security designed to prevent unauthorized access, procedures intended to limit disclosure based upon the ‘need to know,’ and measures that emphasize to recipients the confidential

This list provides examples of available measures and is not intended to be exhaustive in nature. Thus, the level of protection that is reasonable under the facts of a given case may include some, but not necessarily all, of the listed measures. Moreover, a party's effort to secure its trade secrets must be reasonable, not perfect.¹³¹ It is generally recognized "[c]ompanies need not 'guard against the unanticipated, the undetectable, or the unpreventable methods of espionage now available' or create 'an impenetrable fortress.'"¹³²

Whether the efforts parties take to protect their trade secrets are reasonable will depend upon the totality of the circumstances of each case.¹³³ Factors that should be considered include, among other things, the nature and value of the claimed secret, the owner's size and resources, the cost and feasibility of the precautions taken, the cost and feasibility of any precautions not taken, and what is standard in the relevant industry.¹³⁴ Further, it should be recognized the level of precaution an owner must deploy is a fluid concept; hence, precautions that "may be reasonable at one point in time and under one set of circumstances may cease to be reasonable at another time or under other circumstances."¹³⁵

Two decisions by the Iowa courts demonstrate how fluid these concepts can be. In *205 Corp. v. Brandow, The Tavern*, a small Italian restaurant located in West Des Moines, sued its former manager and Mustards, a competing restaurant, for trade secret misappropriation and breach of the duty of loyalty.¹³⁶ The Tavern filed suit after its former manager disclosed the restaurant's secret pizza sauce, pizza crust, and grinder recipes to Mustards.¹³⁷ The Tavern previously terminated the manager's employment, and he began working in a similar capacity for Mustards shortly thereafter.¹³⁸ A jury found in The Tavern's favor and

nature of the information such as nondisclosure agreements, signs, and restrictive legends." RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 cmt. g (1995).

131. *TouchPoint Solutions, Inc. v. Eastman Kodak Co.*, 345 F. Supp. 2d 23, 30 (D. Mass. 2004) (citing *Burten v. Milton Bradley Co.*, 763 F.2d 461, 463 (1st Cir. 1985)).

132. *Pioneer Hi-Bred Int'l v. Holden Found. Seeds, Inc.*, 35 F.3d 1226, 1236 (8th Cir. 1994) (quoting *E. I. duPont deNemours & Co. v. Christopher*, 431 F.2d 1012, 1016–17 (5th Cir. 1970)).

133. 1 MILGRIM & BENSON, *supra* note 51, § 1.04.

134. *Id.*

135. *Id.*

136. *205 Corp. v. Brandow*, 517 N.W.2d 548, 549 (Iowa 1994).

137. *Id.*

138. *Id.*

awarded it over \$300,000 in damages.¹³⁹

On appeal, Mustards argued the recipes the manager disclosed to it were not trade secrets for a variety of reasons.¹⁴⁰ With respect to the pizza crust recipe, Mustards asserted the recipe was not a trade secret because The Tavern routinely disclosed the recipe to its cooks, and “in contrast to other recipes, the crust recipe became known to all employees.”¹⁴¹ Moreover, there was conflicting evidence regarding whether the cooks even regarded the crust recipe as being confidential.¹⁴² Despite The Tavern’s rather blasé attitude toward security, the court found “substantial evidence supported the conclusion that [The Tavern’s] secrecy procedures were reasonable under the circumstances,” and thus, the pizza crust recipe constituted a trade secret under Iowa law.¹⁴³

The United States District Court for the Northern District of Iowa reached a similar conclusion in *Interbake Foods, L.L.C. v. Tomasiello*, a case involving the alleged misappropriation of information concerning the manufacture of ice cream sandwich wafers.¹⁴⁴ Although similar results were reached—in each case recipes were found to be trade secrets—the court in *Tomasiello* applied what was arguably a more exacting standard when determining whether Interbake, the plaintiff, took reasonable efforts to protect its wafer recipes and other alleged trade secrets.¹⁴⁵

Unlike the pizzeria in *205 Corp.*, Interbake took significant steps to protect its trade secrets.¹⁴⁶ Among other things, Interbake implemented a written confidentiality policy, maintained a fence around its production facility, and otherwise limited access to its plant.¹⁴⁷ Despite this, and although it ultimately concluded, on balance, Interbake’s efforts to protect its trade secrets were reasonable, the court was critical of the security measures Interbake implemented—including its written confidentiality

139. *See id.* at 549–50.

140. *See id.* at 550–51.

141. *Id.* at 551 (There was, for example, no evidence The Tavern required its cooks to sign a nondisclosure agreement or that it maintained any type of confidentiality policy.).

142. *Id.*

143. *Id.*

144. *Interbake Foods, L.L.C. v. Tomasiello*, 461 F. Supp. 2d 943, 948 (N.D. Iowa 2006).

145. *Id.* at 966–67.

146. *Id.*

147. *See id.*

policy, which the court referred to as “indolent, at best.”¹⁴⁸ The court was similarly dismayed by Interbake’s failure to “require a *single* employee to sign a covenant not to compete, despite the allegedly highly sensitive nature of Interbake’s wafer manufacturing process.”¹⁴⁹ In contrast, covenants not to compete were not required or even mentioned in *205 Corp.*

The Iowa Supreme Court’s decision in *205 Corp.* is addressed in some detail in *Tomasiello*, and the court ultimately concluded the decision was consistent with its findings regarding the reasonableness of Interbake’s security measures.¹⁵⁰ Even though it paid some lip service to *205 Corp.*, the court plainly expected more from Interbake, a subsidiary of a multibillion dollar corporate conglomerate, than the Iowa Supreme Court expected from The Tavern, a mom-and-pop pizzeria. This difference in treatment suggests the level of precautions a judge or other fact finder considers “reasonable” will, as noted above, vary depending upon a number of factors, including the size and sophistication of the entity seeking trade secret protection. In other words, what is reasonable to protect the secret recipes of a local restaurant may not be sufficient to protect the recipes and manufacturing processes of a large production facility.

The different treatment each court gave to the necessity of having employees sign noncompete agreements further demonstrates differing expectations may exist depending upon the size and sophistication of the party seeking trade secret protection. The court’s criticism of Interbake in *Tomasiello* should not, however, be misread as implying all companies, large or small, must require key employees to sign noncompete agreements if they expect a court to prohibit departing employees from disclosing or using its trade secrets. Indeed, the Iowa Supreme Court rejected this precise argument in *Cemen Tech, Inc. v. Three D Industries*, stating in fairly direct terms, “Whether an employee is subject to a covenant not to compete is not determinative of whether the information gathered through employment constitutes a trade secret.”¹⁵¹

It must also be remembered the *Tomasiello* Court ultimately concluded the information Interbake sought to protect constituted protected trade secrets, although the absence of covenants not to compete

148. *Id.* at 967.

149. *Id.*

150. *Id.* at 965–69.

151. *Cemen Tech, Inc. v. Three D Indus.*, 753 N.W.2d 1, 7–8 (Iowa 2008).

certainly made the determination a closer question in the court's eyes.¹⁵² If any lesson can be learned from *Tomasiello*, it is if a company does not require employees who have access to valuable trade secret information to sign noncompete agreements, that company should be prepared to offer some explanation regarding the reason it failed to take that simple and inexpensive precaution. In addition, the company should be able to point to other significant measures it took to protect the confidentiality of its trade secrets if it expects any court to take its trade secret claims seriously.

The concern expressed in *Tomasiello* regarding Interbake's failure to require at least those employees who had direct access to trade secret information to sign noncompete agreements is consistent with other courts that have been slow to enjoin employees of one company from accepting employment with a competing company absent an enforceable covenant not to compete prohibiting such employment.¹⁵³ This hesitancy was articulated years ago in *E.W. Bliss Co. v. Struthers-Dunn, Inc.*, in which the Eighth Circuit Court of Appeals stated:

Th[e] protection given to trade secrets is a shield, sanctioned by the courts, for the preservation of trust in confidential relationships; it is not a sword to be used by employers to retain employees by the threat of rendering them substantially unemployable in the field of their experience should they decide to resign. This shield is not a substitute for an agreement by the employee not to compete with his employer after the termination of employment. Basically, an employer may not restrict an employee's future employment except by an agreement embodying reasonable terms.¹⁵⁴

Of the protective measures available to companies seeking to protect trade secret information, covenants not to compete and nondisclosure agreements are probably the most prevalent and easiest to implement. Nondisclosure agreements enjoy more favorable treatment under Iowa law

152. *Tomasiello*, 461 F. Supp. 2d at 968.

153. *Int'l Bus. Mach. Corp. v. Seagate Tech., Inc.*, 941 F. Supp. 98, 101 (D. Minn. 1992) ("A claim of trade secret misappropriation should not act as an ex post facto covenant not to compete." (citing *E.W. Bliss Co. v. Struthers-Dunn, Inc.*, 408 F.2d 1108, 1112–13 (8th Cir. 1969))); *see also* *Del Monte Fresh Produce Co. v. Dole Food Co.*, 148 F. Supp. 2d 1326, 1337 (S.D. Fla. 2001) (holding absent actual or threatened misappropriation, courts should not use trade secret laws "as an after-the-fact noncompete").

154. *E.W. Bliss*, 408 F.2d at 1112–13 (citations omitted).

than do noncompetition agreements.¹⁵⁵ Nondisclosure agreements are afforded more favorable treatment because they are not “viewed as restraints of trade which limit an employee’s freedom of movement among employment opportunities.”¹⁵⁶ Unlike noncompete agreements, nondisclosure agreements are, therefore, enforceable under Iowa law even if they lack any geographic or time limitations.¹⁵⁷ However, like noncompetition agreements, nondisclosure agreements are enforceable only if the restrictions contained in the agreement are reasonably necessary for the employer’s business, the restriction does not unreasonably restrict the employee’s rights, and the restriction is not prejudicial to the public interest.¹⁵⁸

VI. HOW ARE TRADE SECRETS MISAPPROPRIATED?

To establish a violation of Iowa’s UTSA, the plaintiff must prove the defendant misappropriated information qualifying as a trade secret.¹⁵⁹ The Iowa UTSA defines “misappropriation” to include the following misconduct:

- a. Acquisition of a trade secret by a person who knows that the trade secret is acquired by improper means.
- b. Disclosure or use of a trade secret by a person who uses improper means to acquire the trade secret.
- c. Disclosure or use of a trade secret by a person who at the time of disclosure or use, knows that the trade secret is derived from or through a person who had utilized improper means to acquire the trade secret.
- d. Disclosure or use of a trade secret by a person who at the time of disclosure or use knows that the trade secret is acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use.
- e. Disclosure or use of a trade secret by a person who at the time

155. *Revere Transducers, Inc. v. Deere & Co.*, 595 N.W.2d 751, 761 (Iowa 1999) (citations omitted).

156. *Id.*

157. *See id.*

158. *Id.* at 762.

159. *Cent. States Indus. Supply, Inc. v. McCullough*, 279 F. Supp. 2d 1005, 1038 (N.D. Iowa 2003).

of disclosure or use knows that the trade secret is derived from or through a person who owes a duty to maintain the trade secret's secrecy or limit its use.

- f. Disclosure or use of a trade secret by a person who, before a material change in the person's position, knows that the information is a trade secret and that the trade secret has been acquired by accident or mistake.¹⁶⁰

That the trade secret be acquired through "improper means" is a common thread running through the various acts of misconduct the Iowa UTSA considers as constituting misappropriation. The Iowa UTSA defines "improper means" to include "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage, including but not limited to espionage through an electronic device."¹⁶¹ Among these listed improper means, that a party disclosed or used trade secret information in violation of a duty he or she had to keep the information secret appears to be the most common source of potential liability. While theft, bribery, misrepresentation, and secrecy are undeniably more intriguing, they are alleged less often as the improper means of misappropriation.

The UTSA does not define the term "espionage." Industrial espionage was, however, at the center of *E. I. duPont deNemours & Co. v. Christopher*, a case in which the Fifth Circuit Court of Appeals considered whether two photographers who took aerial photographs of "a highly secret but unpatented" manufacturing process DuPont was developing, and then sold the pictures to an undisclosed third party, engaged in improper corporate espionage.¹⁶² The court concluded the photographers obtained DuPont's trade secret information through improper means even though the photographers argued "they committed no 'actionable wrong,' . . . conducted all of their activities in public airspace, violated no government aviation standard, did not breach any confidential relation, and did not engage in any fraudulent or illegal conduct."¹⁶³ Applying Texas law, the court rejected the photographer's argument that to be "improper," the means through which trade secret information is obtained "must be a

160. IOWA CODE § 550.2(3) (2009).

161. *Id.* § 550.2(1).

162. *E. I. duPont deNemours & Co. v. Christopher*, 431 F.2d 1012, 1013–14 (5th Cir. 1970).

163. *Id.* at 1014.

trespass, other illegal conduct, or breach of a confidential relationship.”¹⁶⁴

The *Christopher* Court’s conclusion that “improper means” can, under certain circumstances, include methods that are improper—but not necessarily illegal—is consistent with the Restatement approach, which expressly provides “means may be improper . . . even though they do not cause any other harm than that to the interest in the trade secret.”¹⁶⁵ While recognizing that providing a “complete catalogue of improper means is not possible,” the Restatement further instructs that “‘improper means’” includes methods that “‘fall below the generally accepted standards of commercial morality and reasonable conduct.’”¹⁶⁶

What constitutes “generally accepted standards of commercial morality” is, of course, an issue of fact judges or juries must determine based upon the individual facts and circumstances presented to them. The issue, however, relates to the separate inquiry of whether the owner of the trade secret took adequate precautions to protect the information that was allegedly misappropriated. Methods of acquiring information exceeding generally accepted business ethics, and circumventing the reasonable steps an owner can take to protect trade secret information, arguably fall beyond the limits of propriety. As the *Christopher* Court so elegantly observed:

The market place must not deviate far from our mores. We should not require a person or corporation to take unreasonable precautions to prevent another from doing that which he ought not do in the first place. Reasonable precautions against predatory eyes we may require, but an impenetrable fortress is an unreasonable requirement, and we are not disposed to burden industrial inventors with such a duty in order to protect the fruits of their efforts.¹⁶⁷

The duty to keep trade secrets confidential can arise through agreement or by operation of law. The former happens when the party disclosing the confidential information enters into an agreement requiring the party receiving the information to use the information for a designated purpose only and prohibits the receiving party from further disclosing the information.¹⁶⁸ A duty to keep trade secrets confidential arises by operation of law when “the actions of the parties and the nature of their

164. *Id.*

165. *Id.* at 1014–16 (quoting RESTATEMENT (FIRST) OF TORTS § 757 cmt. f (1939)).

166. *Id.* at 1016 (quoting RESTATEMENT (FIRST) OF TORTS § 757 cmt. f (1939))

167. *Id.* at 1017.

168. *See Phillips v. Frey*, 20 F.3d 623, 631 (5th Cir. 1994).

relationship, taken as a whole, establish[] the existence of a confidential relationship.”¹⁶⁹ In those instances, a duty of confidentiality is implied if the relationship between the disclosing and receiving party is such that the receiving party “knew or should have known that the information was a trade secret and the disclosure was made in confidence.”¹⁷⁰

Various relationships can be regarded as confidential under certain circumstances, and those relationships can require a party receiving confidential information to keep that information secret. In his treatise, Professor Milgrim lists the following as potential confidential relationships: employer–employee;¹⁷¹ manufacturer–independent contractor; prospective licensor–licensee; manufacturer–sales agent; supplier–purchaser; and vender–vendee.¹⁷² In each instance, the nature of the relationship is such that a duty of secrecy arises as a matter of law even absent an express agreement to keep the information confidential. However, for a duty of confidence to be implied as a matter of law, the disclosing party must produce the information to further the relationship and the information must be disclosed under circumstances which put the receiving party on notice that the disclosing party regarded the information as confidential.¹⁷³

Of the relationships listed above, the employer–employee relationship is the most common source of trade secret litigation.¹⁷⁴ Most courts, including the Iowa courts, regard the employment relationship as being a confidential one; indeed, the Iowa courts regard the relationship as one between fiduciaries.¹⁷⁵ Given that determination, employees in Iowa are prohibited from disclosing or using trade secret information they obtain during their employment even absent a written agreement to that effect. However, the absence of a written agreement or policy limiting the

169. *Id.* (citing *Hyde Corp. v. Huffines*, 314 S.W.2d 763, 769 (Tex. 1958)).

170. *Id.* at 632 (citations omitted); *see also* 2 ROGER M. MILGRIM & ERIC E. BENSON, MILGRIM ON TRADE SECRETS § 7.01 (2010) (providing the existence of a confidential relationship depends upon “whether . . . [the] recipient of the information disclosed in the relationship knows, or should know, that the information disclosed to it belongs to the discloser and that the disclosure was made in confidence” (citations omitted)).

171. 1 MILGRIM & BENSON, *supra* note 51, § 5.01.

172. 2 MILGRIM & BENSON, *supra* note 170, § 7.01[1]–[5].

173. *Id.* § 7.01.

174. 1 MILGRIM & BENSON, *supra* note 51, § 5.01 (“The great majority of reported trade secret cases arise in the context of the employer–employee relationship.”).

175. *Uncle B’s Bakery, Inc. v. O’Rourke*, 920 F. Supp. 1405, 1430 (N.D. Iowa 1996).

disclosure or use of confidential information places the employer's efforts to maintain the secrecy of that information in doubt and could jeopardize the disclosed information's trade secret status.

In *Pioneer Hi-Bred International v. Holden Foundation Seeds, Inc.*, the Eighth Circuit Court of Appeals dealt with the unique issue of whether a company can be held liable for trade secret misappropriation when there was no direct evidence regarding whether or how the company obtained trade secret information through improper means.¹⁷⁶ The Eighth Circuit held there was sufficient circumstantial evidence of a trade secret violation despite the lack of proof regarding the specific means Holden purportedly used to acquire Pioneer's trade secrets.¹⁷⁷ Despite the lack of specific proof on this critical point, the Eighth Circuit affirmed the lower court's award of over \$46,000,000 in damages.¹⁷⁸

Pioneer alleged Holden, an indirect competitor, misappropriated the genetic makeup of a seed corn line Pioneer developed and then used that information to produce a foundation line used to produce seeds that competed directly with Pioneer's products.¹⁷⁹ Based on scientific testing performed on the various seed lines, the lower court found the seeds Holden produced were derived from Pioneer's misappropriated seed lines.¹⁸⁰ Based on that testing and Holden's inability to credibly explain how it developed the contested seed lines, the district court concluded Holden's seeds were derived from misappropriated Pioneer material.¹⁸¹

On appeal, Holden argued, among other things, Pioneer's trade secret claim was invalid because Pioneer failed to offer sufficient evidence showing Holden misappropriated the genetic makeup of Pioneer's seed corn through improper means.¹⁸² The Eighth Circuit acknowledged this evidentiary shortcoming, but it concluded sufficient circumstantial evidence existed to raise at least an inference of misappropriation—an inference Holden failed to refute.¹⁸³ The specific circumstantial evidence the Eighth Circuit identified included the previously mentioned scientific testing that,

176. *Pioneer Hi-Bred Int'l v. Holden Found. Seeds, Inc.*, 35 F.3d 1226, 1239–40 (8th Cir. 1994).

177. *Id.*

178. *Id.* at 1245.

179. *Id.* at 1228–29.

180. *Id.*

181. *Id.*

182. *Id.* at 1239.

183. *Id.* at 1239–40.

in the court's opinion, "remove[d] the possibility of independent development," Holden's long history of attempting "to obtain Pioneer's genetic material," its faulty record keeping, and the destruction of critical information pertaining to the development of Holden's seed lines.¹⁸⁴ More generally, the court noted "[a]n inference of misappropriation from limited facts is especially warranted in situations such as this where the secret itself is so unique that any form of duplication would probably be improper."¹⁸⁵

Although *Pioneer* may be cited for the general proposition that direct evidence of misappropriation is not necessarily required to prove a trade secret violation, the decision has limited application and should not be projected on factual scenarios involving less compelling circumstantial evidence of misappropriation. It should also be remembered the finding of liability centered upon: (1) uncontroverted expert testimony that, through the use of statistical proof, inexorably linked Holden's product to Pioneer's seed line; and (2) Holden's failure to refute that proof by credibly explaining the process it used to independently develop its product. Absent that proof, it seems certain Pioneer's failure to offer any evidence regarding exactly how Holden misappropriated its trade secret would have diminished its chances of success before the district court and, if not there, certainly before the Eighth Circuit.

VII. DOES THE UTSA PROTECT THREATENED MISAPPROPRIATIONS OF TRADE SECRETS?

The Iowa UTSA prohibits the mere "[a]cquisition of a trade secret by a person who knows that the trade secret is acquired by improper means."¹⁸⁶ Thus, to establish a trade secret misappropriation claim, a "plaintiff need not show that the defendant actually used the secret."¹⁸⁷ The extent to which the trade secret information was actually used is relevant in determining what damages, if any, the plaintiff sustained—not whether there was a misappropriation in the first instance.¹⁸⁸

One of the most interesting issues in Iowa trade secret law is whether a company can obtain an injunction to prevent the threatened use or disclosure of use of a trade secret absent specific evidence the company's

184. *Id.*

185. *Id.* at 1240 (citations omitted).

186. IOWA CODE § 550.2(3)(a) (2009).

187. *EFCO Corp. v. Symons Corp.*, 219 F.3d 734, 741 (8th Cir. 2000) (citing IOWA CODE § 550.2(3) (2000)).

188. *Id.* (citing IOWA CODE § 550.4 (2000)).

trade secrets are actually being used or disclosed. This question typically arises when an employee who had access to valuable trade secret information resigns his or her employment to accept the same, or similar, role with a competing company.¹⁸⁹ In those situations, the company seeking injunctive relief may not only request the court to enjoin the departing employee from using or disclosing its trade secrets, it may also ask the court to enjoin the departing employee from working for its competitor altogether.¹⁹⁰ In those situations, the issue typically is not whether the employee actually possesses trade secret information—that is usually conceded—but whether there is enough of a threat of future disclosure to prevent the employee from working for the competing company at all.¹⁹¹

The Iowa Code permits the owner of a trade secret to seek injunctive relief for the “actual or threatened misappropriation” of a trade secret.¹⁹² The Iowa Supreme Court has yet to determine what evidence must be presented to demonstrate the threatened use or disclosure of trade secrets. However, each of Iowa’s federal courts has addressed the issue, and somewhat surprisingly, both courts have enjoined former employees from continuing their employment with a competing company.¹⁹³

In *Uncle B’s Bakery, Inc. v. O’Rourke*, the court applied what is commonly referred to as the “inevitable disclosure doctrine” to enjoin Kevin O’Rourke, Uncle B’s former production manager, from accepting similar employment with Brooklyn Bagel Boys, a competing company.¹⁹⁴ Even though O’Rourke promised to keep the trade secret information he knew confidential, and even though Brooklyn disavowed any interest in, or need for, the information O’Rourke had acquired, the court concluded a sufficient threat of disclosure existed to enjoin O’Rourke from continuing his employment with Brooklyn.¹⁹⁵ The court’s decision was based upon the unique nature of the information O’Rourke possessed, the similarity between O’Rourke’s new and former positions, and the competitive nature

189. See, e.g., *Uncle B’s Bakery, Inc. v. O’Rourke*, 920 F. Supp. 1405, 1420–21 (N.D. Iowa 1996).

190. *Id.*

191. *Id.*

192. IOWA CODE § 550.3(1) (2009).

193. See *Barilla Am., Inc. v. Wright*, No. 4-02-CV-90267, 2002 WL 31165069, at *13 (S.D. Iowa July 5, 2002); *Uncle B’s Bakery*, 920 F. Supp. at 1441.

194. *Uncle B’s Bakery*, 920 F. Supp. at 1434 n.17, 1435–36.

195. *Id.* at 1435–38.

of the two businesses.¹⁹⁶ In addition, the court recognized it would be difficult, if not impossible, for O'Rourke to separate information that was part of "the fund of general knowledge" O'Rourke accumulated during his employment with Uncle B's—which was usable—from other, more specific information that arguably constituted a protected trade secret.¹⁹⁷

Another Iowa district court followed a somewhat different approach, yet reached the same result, in *Barilla America, Inc. v. Wright*, an unpublished opinion.¹⁹⁸ In that case, Jerry Wright, the plant manager of Barilla's Ames, Iowa production facility, tendered his resignation and accepted a similar position for American Italian Pasta Company (AIPC), one of Barilla's competitors.¹⁹⁹ During his employment with Barilla, "Wright was exposed to a large amount of Barilla's proprietary information," including detailed and confidential information regarding Barilla's manufacturing processes, technical information, research efforts, and financial data.²⁰⁰ Much of that information was stored on CDs and in notebooks, some of which Wright imprudently took with him when he left his employment with Barilla.²⁰¹ Although it had no specific evidence Wright had disclosed or used any of the trade secret information he obtained during his employment, Barilla requested the court to enjoin Wright from continuing that employment, arguing the disclosure of its trade secrets was both threatened and inevitable.²⁰²

In his opinion, Judge Pratt discussed at length the inevitable disclosure doctrine and observed at least one other court took a different course, finding the doctrine was "too prophylactic."²⁰³ The court in *Del Monte Fresh Produce Co. v. Dole Food Co.* applied an "inevitability-plus" rule as well as a separate-but-related standard referred to as the "threatened disclosure doctrine."²⁰⁴ Under these heightened standards, a former employer must not only show disclosure is inevitable, but the employer must also show "a substantial threat of impending injury" is

196. *Id.*

197. *Id.* at 1435.

198. *Wright*, 2002 WL 31165069, at *1.

199. *Id.* at *3–4.

200. *Id.* at *2–3.

201. *Id.* at *3–4.

202. *Id.* at *6.

203. *Id.* at *8 (citing *Del Monte Fresh Produce Co. v. Dole Food Co.*, 148 F. Supp. 2d 1326 (S.D. Fla. 2001)).

204. *Del Monte*, 148 F. Supp. 2d at 1338–39.

present to enjoin a former employee from working for a competitor.²⁰⁵ “Merely possessing trade secrets and holding a comparable position with a competitor” is not sufficient.²⁰⁶

Following the *Del Monte* Court’s lead, the court in *Wright* articulated a “stricter” inevitable disclosure standard that demanded a company seeking to prevent a former employee from working for a competitor prove: (1) the employee obtained or had access to important trade secret information; (2) the employee now holds a comparable position with a competitor; and (3) the employee “would be able to remember the trade secret information in a usable form.”²⁰⁷ A more rigorous standard was warranted because, as the court observed, the former employee was “being required to give up a substantial right . . . and a more searching analysis should be required before [that right] is taken away.”²⁰⁸

After reviewing all of the evidence presented, the court in *Wright* concluded a sufficient threat of disclosure existed to enjoin Wright from working for AIPC, Barilla’s competitor.²⁰⁹ This threat was real and imminent because of the volume of trade secret information Wright took with him when he left his employment with Barilla, some of which Wright had yet to return, and because of other “troubling” conduct Wright engaged in before leaving Barilla.²¹⁰ The court reviewed Wright’s conduct, as well as the somewhat dubious explanations Wright proffered for his actions, and found Wright was not credible and “there [were] simply too many indications that Wright may use [Barilla’s trade secret information] to further his position at AIPC.”²¹¹ The court’s finding that Wright was not credible proved to be determinative as the court also found: (1) “the testimony [did] not show that Wright retained the trade secret information he was exposed to at Barilla” and (2) Barilla failed to make the connection between Wright’s exposure to trade secrets and “to what he actually remembered, or should have remembered, to how he could use it at AIPC.”²¹²

The Northern District Court of Iowa had another opportunity to

205. *Id.* at 1338 (citations omitted).
206. *Id.* (citations omitted).
207. *Wright*, 2002 WL 31165069, at *10.
208. *Id.*
209. *Id.* at *13.
210. *Id.* at *11–12.
211. *Id.* at *12.
212. *Id.* at *10.

apply the inevitable disclosure doctrine in *Interbake Foods, L.L.C. v. Tomasiello*, a case discussed in detail in Part V of this Article.²¹³ In *Tomasiello*, the court agreed with the approach applied in *Wright* and applied a heightened inevitable disclosure standard in rejecting Interbake's argument that it was inevitable Tomasiello would disclose to BoDeans, Tomasiello's subsequent employer and Interbake's competitor, the trade secret information he obtained during his employment with Interbake.²¹⁴ The court observed the inevitable disclosure doctrine was just one way of proving a threatened disclosure, and to enjoin an employee from working with a competitor—as opposed to simply enjoining the employee from disclosing what he or she knows—the moving party must show “a substantial threat of impending injury.”²¹⁵

Applying this standard, the court enjoined Tomasiello from using or disclosing any of the trade secret information he obtained during his employment with Interbake, but it did not enjoin Tomasiello from continuing his employment with BoDeans.²¹⁶ Tomasiello was not enjoined from continuing his employment largely because the evidence showed the trade secret information Tomasiello knew was of limited value to BoDeans, which had independently developed its own production methods that were demonstrably different from Interbake's methods.²¹⁷ More importantly, the evidence indicated Interbake failed to prove Tomasiello took, in a useable form, any of the trade secret information to which he had access during his prior employment.²¹⁸ A substantial threat of pending injury was not proven given those findings.²¹⁹

The heightened inevitability standard applied in *Wright* and later in *Tomasiello* is consistent with a growing number of decisions from courts that have been slow to enjoin employees from working with competing companies absent a showing of actual disclosure or, in the least, threatened disclosure that is both concrete and immediate.²²⁰ This reluctance to enjoin

213. See *supra* Part V.

214. *Interbake Foods, L.L.C. v. Tomasiello*, 461 F. Supp. 2d 943, 973–74 (N.D. Iowa 2006).

215. *Id.* at 973 (quoting *Del Monte Fresh Produce Co. v. Dole Food Co.*, 148 F. Supp. 2d 1326, 1337–38 (S.D. Fla. 2001)).

216. *Id.* at 980.

217. *Id.* at 973–74.

218. *Id.* at 974.

219. *Id.* at 974–75.

220. See, e.g., *Del Monte*, 148 F. Supp. 2d at 1337; *H&R Block E. Tax Servs., Inc. v. Enchura*, 122 F. Supp. 2d 1067, 1074–76 (W.D. Mo. 2000); *EarthWeb, Inc. v.*

is based, in part, upon an aversion against converting an obligation to keep trade secret information confidential into what amounts to a “de facto” noncompete obligation. To address that concern, at least one court has concluded the inevitable and threatened disclosure doctrines should be applied, and injunctive relief issued, only in those rare instances in which the threat of disclosure is both real and imminent.²²¹ Iowa’s other courts will, in all likelihood, apply this rule in future cases.

VIII. WHAT CAN A COMPANY DO WHEN ITS TRADE SECRETS ARE, OR MAY BE, MISAPPROPRIATED?

If a company believes another has misappropriated or might misappropriate its trade secrets, the most effective thing it can do is seek injunctive relief prohibiting initial or further misappropriation. Seeking immediate injunctive relief is consistent with the Iowa UTSA, which specifically authorizes “[t]he owner of a trade secret” to “petition the district court to enjoin an actual or threatened misappropriation.”²²² In Iowa, obtaining immediate injunctive relief means obtaining a temporary injunction under Iowa Rule of Civil Procedure 1.1502.²²³ In United States District Court it means, depending upon the urgency, obtaining either a temporary restraining order under Federal Rule of Civil Procedure 65(b) or a preliminary injunction under Rule 65(a), or both.²²⁴

While the federal and state standards for obtaining preliminary injunctive relief differ, they embody some of the same principles. The factors addressed under the federal standard include: (1) the movant’s probability of success on the merits; (2) the threat of irreparable harm to the movant absent the injunction; (3) the balance between the harm and the injury the injunction’s issuance would inflict on other interested parties; and (4) the public interest.²²⁵ In Iowa, a party seeking a temporary

Schlack, 71 F. Supp. 2d 299, 310 (S.D.N.Y. 1999); *Computer Scis. Corp. v. Computer Assocs. Int’l, Inc.*, Nos. CV 98-1374-WMB SHX, CV 98-1440-WMB SHX, 1999 WL 675446, at *16 (C.D. Cal. Aug. 12, 1999); *Bridgestone/Firestone, Inc. v. Lockhart*, 5 F. Supp. 2d 667, 682 (S.D. Ind. 1998).

221. *EarthWeb*, 71 F. Supp. 2d at 310 (“[I]n its purest form, the inevitable disclosure doctrine treads an exceedingly narrow path through judicially disfavored territory. Absent evidence of actual misappropriation by an employee, the doctrine should be applied in only the rarest of cases.”).

222. IOWA CODE § 550.3(1) (2009).

223. *See* IOWA R. CIV. P. 1.1502.

224. *See* FED. R. CIV. P. 65(a)–(b).

225. *Dataphase Sys., Inc. v. C L Sys., Inc.*, 640 F.2d 109, 113 (8th Cir. 1981); *see* *Uncle B’s Bakery, Inc. v. O’Rourke*, 920 F. Supp. 1405, 1422–23 (N.D. Iowa 1996).

injunction must establish: (1) an invasion or threatened invasion of a right; (2) substantial injury or damages will result unless the request for an injunction is granted; (3) no adequate legal remedy is available;²²⁶ and (4) the likelihood of success on the merits.²²⁷

The Iowa UTSA authorizes the issuance of injunctive relief in response to the actual or potential misappropriation of trade secrets.²²⁸ Thus, an injunction can be issued when the threat of an inadvertent disclosure exists or the eventual disclosure of a trade secret is inevitable.²²⁹ A company whose trade secrets are misappropriated can also recover any actual damages it sustains or obtain some type of royalty payment from the other party.²³⁰ The actual damages the company can obtain are discussed in more detail below.

IX. WHAT LEGAL REMEDIES ARE AVAILABLE TO A COMPANY WHEN ITS TRADE SECRETS ARE MISAPPROPRIATED?

In addition to injunctive relief, the Iowa UTSA also permits a prevailing plaintiff to recover damages including “the actual loss caused by the misappropriation[] and the unjust enrichment caused by the misappropriation which is not taken into account in computing the actual loss.”²³¹ As an alternative remedy, the prevailing plaintiff may recover damages “measured by imposition of liability for a reasonable royalty.”²³² If a willful and malicious misappropriation is proven, the court is authorized to award exemplary damages in an amount not exceeding twice the actual damages or royalty payments that are awarded.²³³ Reimbursement for attorney’s fees incurred is also available to either side

226. Skow v. Goforth, 618 N.W.2d 275, 277–78 (Iowa 2000).

227. Max 100 L.C. v. Iowa Realty Co., 621 N.W.2d 178, 181 (Iowa 2001).

228. IOWA CODE § 550.3(1) (2009).

229. *E.g., Uncle B’s Bakery*, 920 F. Supp. at 1435 (enjoining former plant manager of plaintiff from both disclosing trade secrets and working for a competitor when it was likely the former employee would use trade secret information he possessed in his new employment); *Norand Corp. v. Parkin*, 785 F. Supp. 1353, 1355 (N.D. Iowa 1990) (holding employee was enjoined from working for a competitor); *see Rocklin Mfg. Co. v. Tucker*, No. 00-0797, 2001 WL 1658676, at *2 (Iowa Ct. App. Dec. 28, 2001); *see also PepsiCo, Inc. v. Redmond*, 54 F.3d 1262, 1270–71 (7th Cir. 1995) (upholding a lower court decision temporarily enjoining an employee from disclosing the trade secrets of a former employer).

230. IOWA CODE §§ 550.3(2), 550.4(1) (2009).

231. *Id.* § 550.4(1).

232. *Id.*

233. *Id.* § 550.4(2).

under certain circumstances.²³⁴

Determining actual damages in trade secret misappropriation cases can be difficult and usually requires the testimony of a qualified expert. When sufficient proof is available, the damages can be equal to lost profits based on market analysis.²³⁵

A reasonable royalty payment, like those typically awarded in patent infringement cases, is also a potential remedy.²³⁶ In determining what royalty is appropriate, the judge or jury must estimate the amount the defendant would be willing to pay to use the trade secret and the amount the plaintiff would be willing to accept to sell or license the secret.²³⁷ Furthermore,

[d]etermining a reasonable royalty is analogous to a jury's determination of a proper amount of damages for pain and suffering in a personal injury suit. Like reasonable royalties, pain and suffering cannot be measured by an exact mathematical formula. . . . Rather, pain and suffering rest in the sound discretion of the jury based upon a fair and impartial consideration of all the evidence.²³⁸

X. WHAT IS THE FUTURE OF IOWA TRADE SECRET LAW?

New technologies emerge with increasing rapidity, forever expanding the limits of what is both possible and feasible. Underlying this growth is the inventor's ability to build upon theories and concepts previously discovered and to not waste valuable time and resources forever reinventing the wheel. True growth happens when biologists, chemists, engineers, computer scientists, and other creative individuals are free to build upon existing technologies and know-how, and when they are not unduly hampered by arcane or overly rigid claims of ownership. Equally critical to true growth is the inventor's right to retain and control what she

234. *Id.* § 550.6.

235. *See* EFCO Corp. v. Symons Corp., 219 F.3d 734, 741–42 (8th Cir. 2000) (explaining expert testimony comparing EFCO's revenue erosion to Symons's revenue gains was sufficient to allow jury to determine the extent of EFCO's damage); Basic Chems., Inc. v. Benson, 251 N.W.2d 220, 233 (Iowa 1977) (noting changes in business volume, “especially in the way of net profits,” after an actionable wrong “is competent and instructive evidence” of the actual damages a party has sustained (quoting DeVries v. Starr, 393 F.2d 9, 20 (8th Cir. 1968))).

236. *See, e.g.,* Olson v. Nieman's, Ltd., 579 N.W.2d 299, 310–13 (Iowa 1998).

237. *Id.*

238. *Id.* at 310 (citing Oldsen v. Jarvis, 159 N.W.2d 431, 434 (Iowa 1968)).

invented or developed—to prevent others from misappropriating what she developed and has intentionally kept out of the public domain.

Striking a proper balance between the competing interests in promoting the free exchange of ideas and protecting legitimate property rights is the challenge underlying trade secret law in Iowa and elsewhere. In applying the law, courts everywhere must be cognizant that the definition of what constitutes a trade secret must evolve as new technologies emerge and develop. Concepts not readily ascertainable through proper means today may be readily ascertainable tomorrow. Similarly, steps necessary to keep an idea or discovery secret today may be ineffective tomorrow. In addition, courts must continue to appreciate what constitutes a trade secret depends largely upon the specific facts of each case and few generalities can or should be drawn from the existing case law.