

7-2024

Standards in Assessing Notice of Reasonable Security Measures in Trade Secret Law

Tazeen Hussain

Follow this and additional works at: https://repository.uclawsf.edu/hastings_science_technology_law_journal



Part of the [Science and Technology Law Commons](#)

Recommended Citation

Tazeen Hussain, *Standards in Assessing Notice of Reasonable Security Measures in Trade Secret Law*, 15 HASTINGS SCI. & TECH. L.J. 131 (2024).

Available at: https://repository.uclawsf.edu/hastings_science_technology_law_journal/vol15/iss2/2

This Article is brought to you for free and open access by the Law Journals at UC Law SF Scholarship Repository. It has been accepted for inclusion in UC Law Science and Technology Journal by an authorized editor of UC Law SF Scholarship Repository. For more information, please contact wangangela@uchastings.edu.

Standards in Assessing Notice of Reasonable Security Measures in Trade Secret Law

BY: TAZEEN HUSSAIN*

TABLE OF CONTENTS

Subjectivity from the Plaintiff’s Perspective.....	133
An Objectively Reasonable Defendant	134
How Courts Analyze Reasonable Efforts.....	135
Non-Disclosure Agreements and the Significance of Notice.....	137
Need-to-Know Basis	140
When Notice Fails	142
DTSA: A National Perspective	144
Discrepancies in Oral and Implied Contracts.....	144
Oral Instructions	145
Password Protected and Restricted Access Information and the Defendants’ Knowledge	147
Effects on Future Cases.....	149
Concluding Remarks	150

Every version of trade secret law requires that the plaintiff take reasonable measures to secure the claimed trade secret. But, as this paper will demonstrate, courts have oscillated between an objective standard for that requirement and less consistent subjective standards. This paper proposes that courts adopt a uniform standard in cases where the defendant argues that it was unaware that the information was to be treated as a trade secrets: in such cases, courts should inquire, objectively, whether a reasonable person in the circumstances would have recognized that the information was to be

*J.D. Candidate, Class of 2024, University of California College of the Law, San Francisco. The author would like to thank Professor Charles Tait Graves for his endless support, feedback, and encouragement.

treated as a trade secret based on the security measures the plaintiff employed.

Trade secret law has been shaped with the goal of protecting certain intangible business information unknown to competitors. Whether that information is held by a corporate entity or an individual, the philosophy behind trade secret law is so that companies or individuals can keep their information secret from their competitors so that they can deliver a distinct product or service to consumers.¹

The Uniform Trade Secrets Act (UTSA) was created by the Uniform Law Commission.² The UTSA's definition of a trade secret is "information, including a formula, pattern, compilation, program, device, method, technique, or process that derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."³ In short, the UTSA defines a trade secret as something that is not generally known to others in the field, derives economic value from being a secret, and the trade secret holder takes reasonable efforts, under the circumstances, to maintain that secret.

A similar act, the Defense Trade Secrets Act (DTSA), was signed into law by President Obama in 2016.⁴ The wording in the DTSA is like the UTSA, but instead of the "reasonable under the circumstances" wording, the DTSA's standard is written as "reasonable measures to keep such information a secret."⁵ The goal of both acts is to ensure that trade secrets are protected, but to also limit the scope of what a trade secret could be.

Protecting trade secrets is a significant challenge. As new technologies emerge every year, companies must ensure that their trade secrets are safeguarded. Some of the ways technological companies can keep trade secrets secure is restricting off-site access, use of sufficient encryption, employing software to monitor their employees' computer activity, and automatically shutting off employee access upon departure.⁶ However, there are not clear

1. See Ekaterina G. Long, *The Law of Intangible Assets: The Philosophical Underpinnings of Trade Secret Law in the United States*, 19 SMU SCI. & TECH. L. REV. 125, 125 (2017), <https://scholar.smu.edu/cgi/viewcontent.cgi?article=1036&context=scitech>.

2. See *Trade Secret*, CORNELL L. (May 17, 2023, 9:51 AM) [<https://perma.cc/8AM9-YNH4>].

3. *Id.*

4. See *President Obama Signs Defend Trade Secrets Act Into Law* (May 11, 2016), https://www.cov.com/-/media/files/corporate/publications/2016/05/president_obama_signs_defend_trade_secrets_act_into_law.pdf.

5. 18 U.S.C. § 1836 (2016).

6. See Ian Dibernardo, *Trade secret protection in corporations: best practices*, REUTERS (Apr. 15, 2022, 4:02 AM) [<https://perma.cc/L7CX-9GW7>].

standards established by the courts that illustrate what exactly “reasonable” efforts and measures are under the UTSA and DTSA, respectively.⁷

SUBJECTIVITY FROM THE PLAINTIFF’S PERSPECTIVE

The history of trade secret law in the United States goes back for many decades. In the early 1970s and 1980s, the reasonable efforts prong was analyzed by courts across the nation. Some courts looked at the subjective intent of the plaintiff in analyzing whether reasonable efforts were taken to protect trade secrets. In *University Computing Co. v. Lykes-Youngstown Corp.*, the court viewed reasonable efforts through the plaintiff’s subjective intent.⁸ The court reasoned that “certainly it was undisputed that the UCC viewed the system as a valuable and unique property and used great caution in attempting to preserve its confidentiality.”⁹ In *Metallurgical*, the court determined that the plaintiff took reasonable measures to conceal their proprietary information, furnaces, from all authorized personnel.¹⁰ They were hidden from public view and signs warned people about restricted access.¹¹ There was also a non-disclosure agreement in place.¹² The court stated that “one’s subjective belief of a secret’s existence suggests that a trade secret exists.”¹³ Furthermore, the court said that because security measures cost money, a manufacturer therefore would not incur the costs of security measures if it believed competitors already knew about the information involved.¹⁴

The problem with viewing the reasonable measures analysis solely through the plaintiff’s intentions, is that it disregards the defendant’s understanding of whether the plaintiff’s information should be protected. A plaintiff can implement security measures and require employees to sign non-disclosure agreements, but if the defendant is not completely aware of what the exact information is that needs to be protected, it would be difficult to expect the defendant to keep a company’s confidential information a secret.

Other courts have taken the opposite approach. In a Fifth Circuit case, the court said that even if the plaintiff had the intention to keep the processes

7. Seth J. Welner & John M. Marra, *Defend Trade Secrets Act vs. Uniform Trade Secrets Act: Reasonable Security Measures as Objective or Subjective?*, HOLLAND & KNIGHT (Aug. 6, 2018), <https://www.hklaw.com/en/insights/publications/2018/08/defend-trade-secrets-act-vs-uniform-trade-secrets> [https://perma.cc/KA48-S48Y].

8. *Univ. Computing Co. v. Lykes-Youngstown Corp.*, 504 F.2d 518, 534–35 (5th Cir. 1974).

9. *Id.* at 535.

10. *Metallurgical Indus. Inc. v. Fourtek, Inc.*, 790 F.2d 1195, 1199 (5th Cir. 1986).

11. *Id.*

12. *Id.* at 1205.

13. *Id.* at 1199.

14. *Id.*

and machinery a secret, the intention will be disregarded if there is an absence of proper precautions against disclosure.¹⁵ The court made a compelling statement in the end of the opinion and said “to limit a man in the exercise of his knowledge there must be a strong showing that the knowledge was gained in confidence.”¹⁶ This exemplifies the importance of the defendant’s knowledge and understanding of the confidential essence of the plaintiff’s work and that the plaintiff’s mere intentions, without communicating that intention to the defendant, is not enough. This is also a higher standard than viewing the existence of a trade secret solely through the subjective eyes of a plaintiff.

AN OBJECTIVELY REASONABLE DEFENDANT

Historically, courts have looked at various factors in determining whether the plaintiff took reasonable measures to protect their trade secrets, and this is usually a question of fact.¹⁷ Because this analysis is usually fact-intensive, often there is no national standard as to what would constitute reasonable measures.

Although there is not at outright declaration in the law or in how trade secret cases are usually analyzed, case law suggests that providing notice to the defendants is necessary and that failure to do so may be considered in determining whether the employer has exercised reasonable efforts.¹⁸ Courts across the country emphasize the importance of plaintiffs communicating the existence of their trade secrets through the implementation of various security measures ranging from non-disclosure agreements to password protected files. As practical as this analysis might sound, this leads to varied conclusions because often courts are forced to read into defendants’ minds and try to determine whether reasonable security measures were sufficient to give defendants notice of trade secrets.

However, on the other hand, many courts across the country have found specific notice to employees to be unnecessary because of the nature of the defendants’ job that should have indicated to them that the employees knew about the confidential nature of their work.¹⁹ Although specific notice is not required in these types of cases, there is still an indication that the defendant’s knowledge and understanding of the confidential nature of the plaintiff’s trade secret is an important factor in a court’s analysis.

15. *Wheelabrator Corp. v. Fogle*, 317 F. Supp. 633, 639 (W.D. La. 1970).

16. *Id.* at 638.

17. See JAMES POOLEY, TRADE SECRETS § 1.01 n.1 (2011).

18. *Id.* at §1.01.

19. *Id.*

Providing notice to the defendant is, in my opinion, necessary to analyze whether reasonable measures were taken to protect trade secrets. If the defendant doesn't know they are supposed to keep something a secret, it is difficult to expect employees to protect those secrets. As intuitive and logical as this analysis sounds, at times, courts don't always consider notice as an important factor.²⁰ This, in my opinion, is not the best way to analyze whether a trade secret existed. But because of the lack of a uniform standard across the country, or at least one that can make trade secret analysis a bit more straightforward, courts should make notice to the defendant a determining factor in their analysis as opposed to not analyzing this factor at all.

Therefore, a more proper and rational standard that courts should use in their trade secret analysis is measuring whether the defendant had proper understanding of the existence of a trade secret and viewing this analysis through the lens of an objectively reasonable defendant. This is a far superior standard for courts to use than to completely ignore the significance of notice or to view reasonable measures from a subjective, case by case standard. Although this analysis might still be imperfect, but if courts ask themselves, whether an objectively reasonable defendant would determine from signing a non-disclosure agreement or gaining access to proprietary information through an encrypted file, that there exist specific trade secrets that needed to be protected, it will provide a clearer and more uniform standard.

HOW COURTS ANALYZE REASONABLE EFFORTS

The way courts have historically analyzed reasonable efforts has been very flexible.²¹ Courts usually analyze whether a plaintiff has taken reasonable measures to protect their trade secrets on a case-by-case analysis.²² Reasonableness depends on circumstances and may differ for large and small businesses.²³ In some jurisdictions, for example, courts have viewed the size and nature of the plaintiff's business, the cost that it would incur for additional measures, and the degree to which such measures would decrease the risk of disclosure.²⁴ What may be reasonable measures in one context may

20. *United States Gypsum Company v. LaFarge North American, Inc.*, 508 F. Supp.2d 601, 625 (N.D. Ill. 2007) (summary judgement for the defendant on the grounds that confidentiality markers were not prominent despite there being testimony that the defendants were given specific instructions to not use documents for other projects).

21. *See* Pooley, *supra* note 17, at §1.01.

22. *Id.*

23. *Niemi v. NHK Spring Co., Ltd.*, 543 F.3d 294, 301 (6th Cir. 2008).

24. *In re Innovative Construction Systems, Inc.*, 793 F.2d 875, 884 (7th Cir. 1986).

not necessarily be a reasonable measure in another context.²⁵ Additionally, some jurisdictions only require reasonable measures, not perfection.²⁶

One of the most significant factors, however, that courts sometimes look at is whether the defendant got notice of the confidential nature of the plaintiff's information.²⁷ In a Seventh Circuit case for example, the plaintiff did not require its employees to sign non-disclosure agreements, employee guidelines did not mention the confidential nature of the plaintiff's formulas, and employees were not given exit interviews concerning the confidential nature of the formulas.²⁸ However, the court determined that reasonable precautions were taken because employees were told of the secret nature of the formulas and agreed to keep that information confidential.²⁹ In contrast, the importance of communication is also exemplified in cases where tight security measures were taken, but because the plaintiff did not implement any other security measure, they failed the reasonable measures prong. In *RV Horizons*, the plaintiffs argued that they protected and maintained their lists with the utmost security.³⁰ They stated that the information was password-protected, and access was provided only to a limited number of individuals on an as-needed basis for investor relations.³¹ There was also no evidence of any type of confidentiality agreement, handbook, or training regarding the access to or use of investor lists.³² This indicates that for the court, something additional was needed besides tight security measures to suffice as reasonable efforts.

In *Incase Inc. v. Timex Corp.*, the court determined that the fact that the plaintiff kept its work for private from the world was not sufficient.³³ This was because discretion was considered a normal feature of a business relationship and not a reasonable measure.³⁴ Instead, the court concluded, that there must be affirmative steps to preserve the secrecy of the information as against the party against whom the misappropriation claim is made.³⁵ This exemplifies that for many courts, not only does the plaintiff's degree of

25. *Id.*

26. *International v. Quest Software, Inc.*, 333 F. Supp. 2d 688, 696 (N.D. Ill. 2004).

27. *Univ. Computing Co. v. Lykes-Youngstown Corp.*, 504 F.2d 518, 534 (5th Cir. 1974).

28. *In re Innovative Construction Systems, Inc.*, 793 F.2d 875, 883 (7th Cir. 1986).

29. *Id.* at 884-85.

30. *RV Horizons, Inc. v. Smith*, No. 18-CV-02780-NYW, slip op. at 26 (D. Colo. Nov. 13, 2020).

31. *Id.*

32. *Id.*

33. *Incase Inc. v. Timex Corp.*, 488 F.3d 46, 53 (1st Cir. 2007).

34. *Id.*

35. *Id.*

security efforts matter, but that they must be taken against the defendant.³⁶ Courts have also determined that one who claims that he has a trade secret must exercise eternal vigilance.³⁷ This means constant warnings to defendants and obtaining an agreement, preferably in writing, acknowledging its secrecy and promising to respect it.³⁸ To exclude a secret from the public would not be enough.³⁹ Here, again, what's being emphasized is not the vast amount of security measures, but instead that those measures were taken against the defendant and in essence, communicated to the defendant either through a contract or some sort of verbal instruction.

This exemplifies the importance of notice to the defendants and how heavily this factor weighed in the court's analysis. However, courts overlook the importance of notice in their own analysis, and it is often not clearly recognized under the UTSA.

NON-DISCLOSURE AGREEMENTS AND THE SIGNIFICANCE OF NOTICE

One of the classic examples of what plaintiffs have attempted to qualify as a trade secret are customer lists. In *Morlife Inc., v. Perry*, the defendant was a sales representative at plaintiff's commercial roof repair company.⁴⁰ During this employment at plaintiff's company, he agreed not to use, duplicate, or disclose information about plaintiff's customers if he terminated his employment.⁴¹ Before leaving the company, he took a collection of business cards he collected from P's customer base.⁴² The court found that the plaintiff had made reasonable efforts to keep their trade secrets confidential because the customer information was stored on a computer with restricted access and the defendant had also signed an employment contract with a confidentiality provision expressly referring to its customer names and telephone numbers.⁴³ Although other factors were at play here that influenced the court's decision, such as the how the plaintiff expended a lot of time to build a strong customer list, it can be concluded that a confidentiality agreement as well as storing the customer lists on a computer with restricted access was sufficient to be considered "reasonable efforts" to keep the customer list a secret. From this straightforward case, it can be concluded that

36. *Id.*

37. *J. T. Healy & Son, Inc. v. James A. Murphy & Son, Inc.*, 357 Mass. 728, 738, (1970).

38. *Id.*

39. *Id.*

40. *Morlife, Inc. v. Perry*, 56 Cal. App. 4th 1514, 1518 (1997).

41. *Id.*

42. *Id.*

43. *Id.* at 1523.

a non-disclosure agreement would suffice if there's proper notice to the defendant about the existence of a trade secret.

One interesting thing to note in this landmark case, however, is that the court viewed this analysis through the plaintiff's perspective noting that "based upon the facts of this case, there is no doubt Morlife intended its customer information to remain secret and undertook steps to secure that end."⁴⁴ There is no mention of the defendant's understanding and acknowledgment of a trade secret, although it is implied throughout the analysis. The plaintiff probably did intend to safeguard their customer lists, and this is an important element to consider in trade secret analysis. However, viewing this analysis from the defendant's perspective would allow the court to examine the reasonable measures prong more in depth which would lead to a stronger conclusion.

The importance of notice in non-disclosure agreements is further exemplified in cases where non-disclosure agreements were deemed insufficient. In *Electro-Crat Corp. v. Controlled Motion Inc.*, the court determined that requiring some of its employees to sign confidentiality agreements was not enough.⁴⁵ The court analyzed how a necessary element of trade secret status is proof by the owner of reasonable efforts to maintain secrecy and a showing of mere intention to keep the information a secret is not enough.⁴⁶ The court reasoned that reasonable efforts need to signal to the employees the secret nature of certain information.⁴⁷ Although all of these employees signed confidentiality agreements, the court considered them vague.⁴⁸ This case further demonstrates the importance of notice, and even with a confidentiality agreement in place, if a contract is vague or does not pinpoint to the exact information that needs to be protected, courts will determine that defendants were not given enough notice to truly understand what needs to be protected.

In another interesting case, *Arcor Inc. v. Haas*, the plaintiff attempted to protect his customer lists by having its employees sign and employment and confidentiality agreements.⁴⁹ The court reasoned that because the only security measure that the plaintiff took was to have its employees sign confidentiality agreements, this was not enough.⁵⁰ The fact that the plaintiff presented no evidence that he did "anything more" than require employees to sign a confidentiality agreement impacted the court's ruling.⁵¹ The court

44. *Id.*

45. *Electro-Crat Corp. v. Controlled Motion, Inc.*, 332 N.W.2d 890, 901-902 (Minn. 1983).

46. *Id.* at 892.

47. *Id.*

48. *Id.* at 903.

49. *Arcor, Inc. v. Haas*, 842 N.E.2d 265, 270 (2005).

50. *Id.* at 271.

51. *Id.*

reasoned that had the plaintiff take additional measures, such as limiting access to its customer information by computer password, the court would have concluded differently.⁵² Although there was no evidence of vagueness in the non-disclosure agreements, the court ruled that something additional was required. This, of course, is a rare case, however, it exemplifies how there are discrepancies in analyzing reasonable measures because even though a non-disclosure agreement was in place, the court did not provide a valid ground as to why it was not a reasonable measure.

To further exemplify the discrepancies in the courts, some courts have even ruled that when a defendant refuses to sign a confidentiality agreement, the alleged verbal promise of confidentiality would suffice as a reasonable measure.⁵³ In *Harbor Software, inc. v. Applied Systems, inc.*, the defendant refused to sign a non-confidentiality agreement, but, according to plaintiff, the defendant assured him that “the confidentiality agreement would be part of whatever business agreement was eventually worked out.”⁵⁴ These cases demonstrate that analyzing reasonable efforts is not always clear. In some cases, non-disclosure agreements are not considered enough, but oral statements from the parties or actions are considered reasonable efforts under the circumstances. How courts reach their analysis is not always clear. They often resort to analyzing the subjective understanding of a defendant in each particular case. However, as demonstrated by the cases above, this standard does not always portray uniformity.

As demonstrated through various cases, notice is a determining factor, however deciding whether the defendants got sufficient notice in their non-disclosure agreements is a challenging area for many courts. In *BDT Products, Inc. v. Lexmark Int’l., Inc.*, the Sixth Circuit court determined that the plaintiff releasing information to other companies under a “one-way” non-disclosure agreement that protected only their secrets was fatal, although there was an industry understanding of confidentiality.⁵⁵ Viewing the contract at face-value, the court determined that because the language of the agreements was clear, the understanding of the companies was irrelevant.⁵⁶ This statement, in my opinion, is unsettling particularly because if there was any indication that the defendant in this case, another company, had understanding and notice of the existence of plaintiff’s trade secret and the obligation to protect that secret, then the understanding of the companies should have mattered to the court’s analysis.

52. *Id.*

53. *Harbor Software, Inc. v. Applied Systems, Inc.*, 887 F. Supp. 86, 90 (S.D.N.Y. 1995).

54. *Id.* at 88.

55. *BDT Products, Inc. v. Lexmark Int’l., Inc.*, 124 Fed. Appx. 329, 332-33 (2005).

56. *Id.* at 331.

NEED-TO-KNOW BASIS

Although non-disclosure agreements are standard in many industries, caselaw suggests that plaintiffs have not used non-disclosure agreements for their confidential information, but still have been able to successfully pass the reasonable measures prong on what it means for something to be a trade secret purely because the defendant was specifically informed about confidential nature of the trade secret. In the 1990 case *Courtesy Temporary Services v. Camacho*, the California Court of Appeal affirmed a ruling that the plaintiff's customer information was considered a trade secret because access to the information was divulged to employees only on a as needed basis.⁵⁷ Most importantly, the employees were advised of its confidentiality.⁵⁸ There is nothing from the facts that indicate that there was a confidentiality agreement, indicating that the employees' knowledge and understanding that the information was confidential was the primary reason that the court ruled the way they did.

Other courts have ruled similarly and don't expect high levels of security, particularly for small family businesses. In an Indiana case, the court ruled that the plaintiff took reasonable measure to secure its secrets and this was largely because it trusted its employees to keep its data confidential.⁵⁹ What was particularly interesting about this case is that the court reasoned that even without specific directions or security measures by the plaintiff, the defendant's own security measures contributed to the maintenance of confidentiality.⁶⁰ The record reflected that the defendant locked the data compilation in his toolbox at the end of the day and never allowed other employees to copy the data.⁶¹ Shockingly, the court concluded that these efforts that the defendant took to protect the data compilation were to be attributed to the plaintiff.⁶²

The above case put a huge emphasis on the defendant's knowledge and understanding of the trade secret and going so far as attributing the reasonable efforts the defendant took to the plaintiff. Without the plaintiff implementing any security protocols whatsoever, the court still determined that reasonable measures were taken through the defendant's actions. This case is an example how courts sometimes must almost read the defendant's thoughts in order to determine whether they understood the existence of a trade secret.

57. *Courtesy Temp. Serv., Inc. v. Camacho*, 222 Cal. App. 3d 1278, 1288 (1990).

58. *Id.*

59. *N. Elec. Co. v. Torma*, 819 N.E.2d 417, 428 (Ind. Ct. App. 2004).

60. *Id.*

61. *Id.* at 427.

62. *Id.*

This is further exemplified in *Johns-Manville Corp. v. Guardian Indus. Corp.*, where the court determined that even if the defendants had not been told about that the information was secret, they should have been able to conclude from the very nature of the work that they were doing.⁶³ Although in this case, the defendants did sign a confidentiality agreement, the court reasoned that the defendant was not only aware of the secret and confidential nature of his work, but also responsible for maintaining that secrecy.⁶⁴ This analysis is very similar to the *Torma* case above where the defendant was responsible for the plaintiff's trade secrets and because of that responsibility, the defendant's reasonable efforts were attributed to the plaintiff. What was most astounding about the court's analysis in this case was that the defendant was not even instructed about the existence of confidential information, but the court determined through his actions that he must have known that a trade secret existed. In my opinion, this is not an ideal way to analyze the reasonable measures prong because it forces courts to determine what the defendants are thinking.

Even in cases where defendants have not been expressly informed about the nature of a trade secret, the court has still ruled in the plaintiff's favor.⁶⁵ The court in a Second Circuit case reasoned that educated employees should be aware that the information is not revealed to outsiders or used to the disadvantage of its owners.⁶⁶ The defendants argued that the plaintiff failed to prove that the defendants had any reason to believe that the data was intended to be confidential.⁶⁷ However, the court still held that the defendant must have deduced that unlike the assembly drawings, which were freely circulated to customers, the parts drawings were not.⁶⁸ Additionally, because the defendant was willing to pay for the parts drawings exemplifies that he knew their value and that they hold secrecy.⁶⁹ In this case, there was no evidence that the plaintiff took any measures to protect the parts drawings and the court's conclusion that the defendant should have deduced what was confidential is, in my opinion, not a proper analysis of the reasonable measures prong. It is the plaintiff's responsibility to make a good-faith effort in protecting its trade secrets and if the plaintiff makes no reasonable efforts at all, it is difficult to expect a reasonable defendant in that situation to understand what is deemed confidential.

63. *Johns-Manville Corp. v. Guardian Indus. Corp.*, 586 F. Supp. 1034, 1072-1073 (E.D. Mich. 1938).

64. *Id.* at 1072.

65. *A. H. Emery Co. v. Marcan Prod. Corp.*, 389 F.2d 11, 16 (2d Cir. 1968).

66. *Id.*

67. *Id.*

68. *Id.*

69. *Id.* at 17.

From the above cases, we can conclude that notice and communication to the defendant are important to many courts across the country in reaching their analysis. But because of the lack of a uniform standard under the UTSA, courts are forced to analyze whether defendants have had proper notice of whether something is a trade secret, which can cause discrepancies in the court's conclusions. Therefore, it is not only important for the court to analyze the plaintiff's actions in safeguarding his or her information, but it is vital that courts analyze whether an objectively reasonable defendant would be able to conclude from the plaintiff's security measures that trade secrets need to be protected. This will decrease the number of discrepancies across the country and it will also be easier for the courts to analyze the reasonable measures prong because they wouldn't have to analyze each defendant's knowledge and understanding as much and instead, use a uniform standard.

WHEN NOTICE FAILS

As examined from the cases above, informing the defendants of the existence of a trade secret suffices and at times, even the nature of the defendant's job is sufficient for the defendant to know that the plaintiff's information must be kept a secret. However, there are times when courts decide that there is not enough notice to the defendant.

In an Illinois case, the plaintiff did not require the defendants to sign non-disclosure clauses.⁷⁰ The plaintiff made the argument that no one other than the defendant was exposed to the trade secret, but this was still not considered a reasonable effort to maintain secrecy.⁷¹ The plaintiff had certain secrets related to the dairy industry that they only told the dairy company.⁷² Similarly, they had trade secrets related to the transportation industry that was only told to the transportation-defendants.⁷³ Even then, the court said that because nothing prevented the defendants from sharing this information with others that were not in the industry, there are no reasonable efforts to maintain those secrets.⁷⁴ Even though the plaintiff divided their trade secrets among those with a need to know and depending on their industry, it was still determined that this was not sufficient notice. Contrasting this with *Johns-Manville Corp. v. Guardian Indus. Corp.*, even though it could be argued that because of the nature of the defendant's work, they should have known to keep the plaintiff's information confidential, the court in this case made no such ruling for the plaintiff.

70. *Sw. Whey, Inc. v. Nutrition 101, Inc.*, 117 F. Supp. 2d 770, 780 (C.D. Ill. 2000).

71. *Id.*

72. *Id.*

73. *Id.*

74. *Id.*

Notice to the defendant can be a difficult thing for the courts to conceptualize. The plaintiff in *Gen. Insulation Co. v. King* had, as its policy, to protect their information through an “unspoken rule.”⁷⁵ Even then, the unspoken rule about confidentiality did not constitute a reasonable measure to protect that information and summary judgement was granted to the defendant.⁷⁶ Additionally, even with a non-disclosure agreement in place, courts have found that it was not sufficient notice to the defendant as was held in *Dynamics Research Corp.*⁷⁷ This was because when the defendant was leaving the company, the plaintiffs made no additional mention of the non-disclosure agreement.⁷⁸ Although this is a much older case and the reasoning is a bit unusual, it demonstrates how courts have analyzed notice, which in this case the court said that the non-disclosure agreement did not put the defendant on notice that he was working on trade secrets.⁷⁹ It seems like the nature of the defendant’s job or his role at his company did not constitute enough knowledge and notice about how his work was proprietary to the plaintiff.

In *U.S. Gypsum Co. v. LaFarge North American, Inc.*, the court decided that the plaintiff did not present sufficient evidence supporting that its disclosure to the defendant was done with adequate restrictions.⁸⁰ One of most compelling statements of the court was when it stated that “identifying information as proprietary is not the same as denominating it as confidential.”⁸¹ Information was provided to the defendants under strict conditions of confidentiality.⁸² Even though the defendants were instructed to not use the specific drawings outside of work for the plaintiff, the court said this was not prominent enough.⁸³ Contrasting this with the *Johns-Manville Corp.* case, the nature of the defendant’s job was deemed insufficient to put the defendant on notice of the plaintiff’s confidential information.⁸⁴ This is a clear example of a lack of consistency throughout the country. Although there are many reasons as to why courts rule that reasonable efforts were taken, there should still be a clear standard that courts could follow to allow for more conformity across the country.

75. *Gen. Insulation Co. v. King*, No. 14-08-00633-CV, slip op. at *6 (Tex. App. Jan. 26, 2010).

76. *Id.*

77. *Dynamics Rsch. Corp. v. Analytic Scis. Corp.*, 400 N.E.2d 1274, 1287 (1980).

78. *Id.*

79. *Id.*

80. *See supra* note 20, at 625.

81. *Id.*

82. *Id.*

83. *Id.*

84. *See supra* note 40, at 1528.

Even with a non-disclosure agreement in place or verbal instructions to the defendant, courts might still rule that reasonable measures were not taken by the plaintiff. In many of these cases above, the plaintiff's measures were not being evaluated, rather, it was whether the defendant understood the requirements of confidentiality that was expected of them.

DTSA: A NATIONAL PERSPECTIVE

Discrepancies in Oral and Implied Contracts

The DTSA is new, however, even with the limited caselaw that exists under the DTSA, there are still compelling cases that give insight to how courts view reasonable measures taken by plaintiffs. Many companies implement non-disclosure agreements to protect their trade secret information. However, there are rare cases where parties agree to oral contracts to not share confidential information with third parties. Courts have drawn varying conclusions across the country about whether these oral agreements constitute reasonable measures under the DTSA.

The Ninth Circuit has acknowledged the importance of the idea of giving notice to the defendant about a trade secret. In fact, the court has recognized that “trade secret law is a two-way street: It protects ideas, but it also requires giving notice that the information is in fact a secret so that others do not fall into a “trap” of using information that they think is non-confidential.”⁸⁵ The court speaks about the duty of implied duty of confidentiality and how it is found when the other party has reason to know that the information was in fact confidential.⁸⁶ This standard is particularly important in trade secret law analysis. Not only is it imperative that plaintiffs safeguard their trade secrets, but that the defendant has notice that those secrets need to be protected.

In a California case, *Graduation Solutions LLC v. Luya Enter. Inc.*, the plaintiff entered into an oral agreement with the defendants for them to manufacture plaintiff's graduation apparel at the defendants' facility in China, which plaintiff would then sell in the United States.⁸⁷ The oral agreement provided that the defendants agreed to keep plaintiff's design specifications and other non-public business information confidential, and to not use the information for any other purpose except to manufacture the plaintiff's products.⁸⁸ The plaintiff also alleged that it shared other confidential information including market data, vendor information, customer information, and

85. Carr v. AutoNation, Inc., 798 F. App'x 129, 130 (9th Cir. 2020).

86. *Id.*

87. Graduation Sols. LLC v. Luya Enter. Inc., No. CV191382DMGJPRX, slip op. at 2 (C.D. Cal. May 5, 2020).

88. *Id.*

insider information regarding the graduation apparel industry.⁸⁹ The most important factor to note in this case is that for several years, the parties carried their business relationship according to the terms of the oral agreement, which was never memorialized in writing.⁹⁰

After the plaintiff brought action against the defendants for allegedly selling similar graduation apparel on their websites, the court found that the confidentiality agreement did not need to be written to be considered a reasonable secrecy measure and that verbally telling clients and employees that the information was confidential sufficed as a reasonable measure.⁹¹ A similar route was taken in a North Carolina case which found that the defendant's argument that information was shared with him before a non-disclosure agreement was signed did not stand.⁹² Despite the absence of a formal written confidentiality agreement, there was evidence of an oral agreement between the parties to maintain the confidentiality of the plaintiff's information.⁹³

These cases exemplify how oral agreements are considered reasonable measures to protect trade secrets. This exemplifies the importance of providing notice to the defendant in trade secret analysis and how a written non-disclosure agreement is recommended but not always necessary under the DTSA.

Oral Instructions

Although oral instructions can pass the reasonable measures test under the UTSA, they might not always be considered reasonable efforts in many DTSA cases. In *Charles Ramsey Co., Inc., v. Fabtech-NY LLC*, the plaintiff was a piano hardware manufacturing company.⁹⁴ The company began to develop a variety of novel processes and methods of application, which provided the plaintiff company with the economic edge necessary to maintain its business.⁹⁵ The plaintiff's owner, Trout, told the defendants repeatedly that these methods were sensitive information.⁹⁶ The court concluded that advising employees that certain information is a trade secret can be an

89. *Id.*

90. *Id.*

91. *Id.* at 11.

92. *TaiDoc Tech. Corp. v. OK Biotech Co.*, No. 12 CVS 20909, 2016 WL 1221425, slip op. at 8 (N.C. Super. Mar. 28, 2016).

93. *Id.*

94. *Charles Ramsey Co., Inc. v. Fabtech-NY LLC*, No. 118CV0546LEKCFH, slip op. at 1 (N.D.N.Y. Jan. 21, 2020).

95. *Id.* at 2.

96. *Id.*

example of a proper reasonable measure under the UTSA but that the court found no case under the DTSA in which this measure alone was sufficient.⁹⁷

In another California case, the court found that the plaintiff had shown a likelihood of success on the merits of its federal trade secret.⁹⁸ The court was vague in their analysis about whether reasonable measures were taken or not. Still, the plaintiff instructed the defendant and “anyone else associated” with the plaintiff’s operations that customer, leads and profit information had to be kept a secret.⁹⁹ There is no indication from the facts that there was a written agreement between the two parties, but merely a verbal instruction.

In another case, the plaintiffs asserted that they shared information with the defendants in confidence.¹⁰⁰ The court concluded that the plaintiff sharing the information at issue with nothing more than an expectation of privacy was insufficient to establish that reasonable efforts were taken to protect the information and maintain its secrecy.¹⁰¹ The plaintiff showed no method, plan, or other act by which they attempted to maintain the secrecy of the alleged trade secrets.¹⁰² Contrasting the two cases above, it demonstrates how verbal instructions might suffice in one case, but not in another case.

Although there is not a lot of case law under the DTSA, the cases above illustrate the different conclusions that courts come to regarding verbal instructions. This portrays that the defendant’s subjective understanding of whether something is considered confidential is a factor that the court takes into consideration in its analysis. However, how they measure whether the defendant got notice about the confidential nature of the plaintiff’s materials is not always clear.

Additionally, contrasting the above cases with the standard under the UTSA, it can be observed that there is not a lot of case law under the DTSA where courts have determined that the plaintiff providing the defendant with verbal or oral instructions sufficed as reasonable instructions. Under the UTSA, this was exemplified in *Courtesy Temporary Services, Inc. v. Camacho*, where the court concluded that the plaintiff instructing the defendants on the confidential nature of the plaintiff’s customer list was considered a reasonable measure under the UTSA.¹⁰³

Considering how there is no clear-cut standard for whether oral instructions are considered a reasonable measure, looking at the defendant’s

97. *Id.* at 15.

98. *Perfect Enterprises v. Olmedo*, No. EDCV1900690JAKKKX, (C.D. Cal. May 2, 2019).

99. *Id.*

100. *Krawiec v. Manly*, 811 S.E.2d 542, 549 (N.C. 2018).

101. *Id.*

102. *Id.*

103. *Courtesy Temp. Serv., Inc.*, 222 Cal. App. 3d at 1278, 1288 (1990).

knowledge and understanding of what constitutes a trade secret is a good place for the courts to start their analysis. However, as we've seen with the cases above, the issue with analyzing a defendant's knowledge and understanding of the existence of a trade secret could open the door to courts having to analyze the subjective knowledge of each defendant.

Therefore, a more uniform standard that the courts should employ is analyzing reasonable measures, including oral instructions through the eyes of an objectively reasonable defendant. Courts must ask themselves when they come across cases where the plaintiff verbally instructed the defendant to guard certain information, whether a reasonable defendant, in that case, would be able to understand the importance of not sharing that information with an outside party.

PASSWORD PROTECTED AND RESTRICTED ACCESS INFORMATION AND THE DEFENDANTS' KNOWLEDGE

Password-protected information and restricted access measures are also widespread security efforts that many companies take to protect their trade secrets. However, just because information is encrypted or password-protected, it does not mean the courts will rule in the plaintiffs' favor.

In a Minnesota case, the court held that the plaintiff's security measures were mostly , superficial.¹⁰⁴ In this case, the plaintiffs identified the company's rate sheet history and pricing model as confidential and placed them in a limited-access folder.¹⁰⁵ The court decided that the senior officers disseminated this information to its employees for business use and that the plaintiff company said little about what it did to limit access from that point on.¹⁰⁶ The court emphasized that there was no evidence that it distributed this information to its employees on a need-to-know basis.¹⁰⁷ Additionally, it made no difference to the court that these documents included the label "all pricing information is confidential."¹⁰⁸

The court's analysis highlights the point that the information was not shared with employees on a need-to-know basis, although the documents were labeled as confidential. This indicates that to certain courts, reasonable safety efforts are often not measured by the most extreme security measures taken but by the court's analysis of whether employees got sufficient notice of the confidential nature of the information they were exposed to. The court also said that there was no evidence that the plaintiff held training sessions

104. *Prairie Field Servs., LLC v. Welsh*, 497 F. Supp. 3d 381, 396 (D. Minn. 2020).

105. *Id.*

106. *Id.*

107. *Id.* at 396.

108. *Id.*

for the employees on how to protect company trade secrets.¹⁰⁹ Training sessions, although not uncommon, are a degree ahead of what many companies would employ as a security measure. This exemplifies how courts grapple with the reasonable efforts standard.

Although the defendant's understanding and knowledge of a trade secret is important for many courts' analysis, there are times when courts, viewing this analysis on a case-by-case basis, draw varying conclusions. In *MedQuest Ltd. v. Rosa*, the plaintiff reserved to the defendants' special password access to confidential lists, limited administrative access to the lists, and made it difficult for other employees to print, download, or email the list.¹¹⁰ The court concluded that even if confidential lists were trade secrets, the plaintiff did not demonstrate that they took reasonable measures to maintain their confidentiality because the two defendants did not sign a non-disclosure agreement, for example.¹¹¹ Additionally, although the plaintiffs distributed a policy manual containing a confidential information section that explicitly identified customer lists as confidential, the plaintiff did not allege that the defendants acknowledged these obligations and agreed to be bound by them.¹¹²

MedQuest Ltd. v. Rosa demonstrates an interesting point about the court's analysis of the defendant's knowledge and understanding of the confidential customer and lawyer lists. Although there are enough facts to demonstrate that the plaintiff took reasonable measures to secure their confidential information, the court re-emphasized the importance of the defendants' acknowledgment of their confidential obligations. This case demonstrates the dangers of viewing reasonable measures on a case-by-case basis instead of a more objective standard. If the courts view their analysis through an objective standard, courts will not have to read into the defendants' minds to determine whether defendants received reasonable notice of the existence of a trade secret.

Security measures alone rarely suffice as reasonable measures under the DTSA. However, in a Missouri case, the court found that reasonable measures were taken when plaintiffs put their trade secret in a locked office, available on only one computer, and where the access was granted to only a handful of plaintiff's employees.¹¹³ The defendant in this case downloaded the confidential information onto a USB drive without the plaintiff-company's permission while she was employed by the ETF and receiving a salary

109. *Id.* at 397.

110. *MedQuest Ltd. v. Rosa*, No. 21 CIV. 5307 (PGG), 2023 WL 2575051 at *5 (S.D.N.Y. Mar. 20, 2023).

111. *Id.* at 4.

112. *Id.*

113. *Phyllis Schlafly Revocable Tr. v. Cori*, 512 F. Supp. 3d 916, 932 (E.D. Mo. 2021).

from the ETF.¹¹⁴ The court concluded that a lack of confidentiality agreements did not show that the plaintiff failed to take reasonable measures, particularly because officers of a corporation owe independent fiduciary duties to the corporation to protect trade secrets from disclosure.¹¹⁵

Here, although rare, the court found that the plaintiff took reasonable measures to protect their trade secrets by locking the information on a secured computer, where access was granted to only a few employees. Based on the facts of this case, it can be determined that the defendant purposefully downloaded the confidential information, knowing that the plaintiff deemed it confidential and proprietary. It is implied from this analysis that the defendant had sufficient notice of the confidential nature of the information, which was imperative to the court's analysis.

Throughout the country, plaintiffs take varying reasonable measures to protect their trade secrets. Ranging from non-disclosure agreements to password-protected information, a lot of the time, this standard is not difficult to meet. However, there are cases where the courts conclusion comes much to a surprise. Sometimes, high-level security measures are not deemed enough, but oral agreements suffice as reasonable measures. The commonality in all these cases is the court's judgment of whether the defendant was given sufficient notice through these security measures about the existence of a trade secret.

The importance of communicating to the defendant about the existence of a trade secret is the true standard of the reasonable measure requirement under the DTSA. However, the fact that concept is almost nowhere to be found in either the statute or caselaw is quite dangerous and can lead to unexpected and far-off conclusions. Therefore, to make this standard clearer, the reasonable measures prong should be viewed through an objectively reasonable defendant.

EFFECTS ON FUTURE CASES

If courts began viewing the reasonable measures prong through an objectively reasonable defendant, it is hard to conclude whether this will benefit the plaintiff or the defendant.¹¹⁶ From a recent report on trade secret statistics, between 2015 and 2017, following the enactment of the Defend Trade Secret Act, trade secret filings rose 30%.¹¹⁷ Even with the rise of the global

114. *Id.* at 922.

115. *Id.* at 932.

116. Trade Secret Litigation Report 2021, LEX MACHINA, at 22:55 (June 24, 2021), <https://lexmachina.com/media/press/webcasts/webcast-trade-secret-litigation-2021/?aliId=eyJoiRfWvUTBOQnFHdWZ0V0RsZU-ciLCJ0IjoiQkczd20wQ0ZUZ2JrYjZyR3I5d1Btdz09In0%253D>.

117. *Id.* at 4.

pandemic, trade secret filings have remained steady even with large-scale international shutdowns.¹¹⁸ Additionally, looking at the cases on the merits, plaintiffs won at trial over four times as often as defendants (114 cases to 28).¹¹⁹ However, defendants are more likely to win during summary judgment (96 cases to 67).¹²⁰ In 114 cases terminated over the five-year time period, courts found a failure to identify a trade secret such that the claim could not go forward.¹²¹

From these statistics, we can conclude that trade secret filings are not going away any time soon and in fact, are continuing to rise. Although implementing a new standard, such as viewing reasonable measures through an objectively reasonable defendant, might not change the outcome of trade secret cases, it is an important conversation to have and something to consider. A small change that could occur, for example, would be that courts would more likely find that the defendant, being an objective and reasonable person, should have known that the verbal instructions or non-disclosure agreements were enough and were the plaintiff's way of communicating that a trade secret existed. If this is the case, then it might be harder for defendants, especially during summary judgement to argue that they were not given sufficient notice or that the plaintiff did not take reasonable measures.

As courts have recognized trade secrets as property over the years, it is no surprise that plaintiffs are more likely to win at trial. Perhaps this standard would only make it easier for plaintiffs to assert a trade secret claim, but it is difficult to make that conclusion. It could present challenges to defense attorneys who might have a hard time arguing against the objective, reasonable person standard. However, reasonable measures are only one prong in the trade secret analysis and therefore, it might not present any major, impactful changes to the current trade secret litigation regime.

CONCLUDING REMARKS

After reading many UTSA and DTSA cases, giving notice to the defendant is an important standard to measure reasonable efforts and an important one too. However, how courts measure whether a defendant received notice is sometimes very unclear and can cause inconsistencies in the court's decisions. There are cases where verbal instructions were considered enough, but in other cases, tight security measures and non-disclosure agreements were not considered to hold to the standard of reasonable measures. Although no method is going to be perfect, creating a standard will be helpful

118. *Id.*

119. *Id.* at 18.

120. *Id.*

121. *Id.*

for the courts in determining whether the defendant knew that they had a responsibility to keep the plaintiff's materials and information a secret. If the defendant in a trade secret case argues that they were unaware that the information they had access to was to be treated as a trade secret, courts should inquire whether a reasonable person in their circumstances would have recognized that the information was to be treated as a trade secret based on the security measures the plaintiff employed.
