Trade Secrets: 10 Keys to Successful Litigation

by Jessica Brown and Tafari Lumumba

Trade secrets litigation is growing exponentially in some jurisdictions, and companies can find themselves on either side of the issue: seeking to protect trade secrets from being exploited by departing employees or a competitor, or facing suits when their employees take or improperly use confidential information from a former employer or competitor. This article describes 10 keys to successful trade secrets litigation for practitioners without significant experience in this area.

Trade secrets litigation touches a diverse range of corporate actors. Companies can be either plaintiffs suing to protect their proprietary information or defendants rebutting accusations of stealing a competitor's "secret sauce." Individuals starting a new company or accepting a promising job offer can be subject to litigation if they take their former employer's alleged trade secrets to the new venture. With trade secrets theft constituting an estimated 1% to 3% of gross domestic product in the United States,[1] and trade secrets litigation growing "exponentially" in some jurisdictions,[2] corporate actors would be wise to prepare to play offense and defense in this space.

The hypothetical plaintiff in a trade secrets action should consider who could target company intellectual property. Potential perpetrators include (1) current and former employees, (2) competing companies, (3) foreign governments, (4) business partners, and (5) common criminals (hackers, fraudsters, etc.). Hypothetical defendants, on the other hand, should consider who could be high-risk targets for a trade secrets lawsuit. These persons include (1) new hires with third-party information—and their employers, (2) companies hiring "teams" of employees, and (3) joint venture partners.

Despite highly publicized cases of thefts allegedly perpetrated by foreign nations,[3] most cases involve persons known to the trade secrets owner.[4] An empirical study of trade secrets litigation in state and federal courts identified most alleged misappropriators as business partners, current employees, and former employees.[5] Indeed, half of employees surveyed in a 2013 study admitted to having taken company data from former employers and 40% planned to use that data at their new jobs.[6]

If a litigant is armed with knowledge of the law and best litigation practices, there are indeed tangible steps that can be taken to secure an advantage in a trade secrets lawsuit. This article first provides a brief overview of how trade secrets and misappropriation are defined under Colorado law. Then it offers practice tips for when litigation moves from a hypothetical risk to a bet-the-company reality.

What Are Trade Secrets?

The Colorado Uniform Trade Secrets Act (CUTSA) defines a "trade secret" as:

> the whole or any portion or phase of any scientific or technical information, design, process, procedure, formula, improvement, confidential business or financial information, listing of names, addresses, or telephone numbers, or other information relating to any business or profession which is secret and of value. To be a "trade secret" the owner thereof must have taken measures to prevent the secret from becoming available to persons other than those selected by the owner to have access thereto for limited purposes.[7]

Colorado courts consider the following factors to determine whether a trade secret exists:

Coordinating Editor

John M. Husband, Denver, of Holland & Hart LLP—(303) 295-8228, jhusband@hollandhart.com

About the Authors

Jessica Brown is a litigation partner at Gibson, Dunn & Crutcher and a member of the firm's Labor and Employment and Class Action practice groups. She has experience defending nationwide and statewide class and collective actions, and has tried and mediated non-class claims before federal judges and arbitrators across the country. She is the current president of the Colorado Women's Bar Association—jbrown@gibsondunn.com. Tafari Lumumba is a litigation associate at Gibson, Dunn & Crutcher and a member of the firm's General Commercial Litigation, Securities Litigation, and White Collar Defense Investigations practice groups—tlumumba@gibsondunn.com. Jessica is grateful for Tafari's tremendous assistance in preparing this article.

Labor and Employment Law articles are sponsored by the CBA Labor and Employment Law Section to present current issues and topics of interest to attorneys, judges, and legal and judicial administrators on all aspects of labor and employment law in Colorado.

1) the extent to which the information is known outside the business;
2) the extent to which it is known to those inside the business (i.e., by the employees);
3) the precautions taken by the holder of the trade secret to guard the secrecy of the information;
4) the savings effected and the value to the holder in having the information as against competitors;
5) the amount of effort or money expended in obtaining and developing the information; and
6) the amount of time and expense it would take for others to acquire and duplicate the information.[8]

With these criteria in mind, Colorado courts have found trade secrets to encompass myriad categories of information, including customer lists,[9] candidate data for a recruitment agency (including compiled employment histories and job qualifications),[10] and an "Operations and Procedures" manual for franchisees.[11] A Colorado court also ruled that a plaintiff sufficiently pleaded that "login information for profiles" and lists of MySpace "friends" were trade secrets for the purpose of surviving a motion to dismiss.[12]

In other jurisdictions, courts have found formulas,[13] designs,[14] methods,[15] plans,[16] and even information regarding what does not work (knowledge "developed negatively") to merit trade secrets protection.[17] And similar to the MySpace friends list case,[18] plaintiffs in other jurisdictions have also explored social media trade secrets theories, litigating to protect a party's LinkedIn contacts[19] and a company's 17,000 Twitter followers.[20]

What Is Misappropriation?

Misappropriation liability under CUTSA turns on whether a party employs, has knowledge of, or should have knowledge of improper means in the acquisition, disclosure, or use of trade secrets. "Improper means" under the statute includes "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means."[21]

The statute notably does not require that the trade secrets be *used* for liability to attach. If a person merely acquires a trade secret while knowing (or having reason to know) that the trade secret was "acquired by improper means," CUTSA finds liability.[22] Similarly, a party can be held liable for disclosing or using a trade secret if it did the following:

1) used improper means to acquire knowledge of the trade secret; or
2) at the time of disclosure or use, knew or had reason to know that such person's knowledge of the trade secret was:
   a) derived from or through a person who had utilized improper means to acquire it;
   b) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or
   c) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use.[23]

Keys to Successful Trade Secrets Litigation

When embarking on trade secrets litigation, whether as a plaintiff or a defendant, it is useful to have in mind the 10 keys to success that follow.

Key #1—Secure, Collect, and Review Electronic Evidence

Federal courts have expressed varying standards regarding when the obligation to preserve documents begins. A Colorado federal district court held that putative litigants must "preserve documents that may be relevant to pending *or imminent* litigation."[24] Once obligations begin, counsel for corporate litigants should circulate a notice (i.e., a document retention notice or "litigation hold") to employees with potentially discoverable information. Counsel should describe the litigation, the potential locations of discoverable documents (laptops, smart phones, desktops, filing cabinets, etc.), the types of materials covered (e.g., emails, text messages, network documents), and the subject matter of the information that should be retained.[25]

Corporate litigants should also ensure that automatic document destruction protocols are suspended. Failure to preserve relevant evidence—even if pursuant to an automatic document destruction protocol—may result in an "adverse inference" instruction allowing jurors to presume the missing evidence was unfavorable to the sanctioned party.[26]

While potential court-ordered sanctions should be sufficient incentive for all litigants to preserve discoverable data, companies in a trade secrets action should immediately collect electronic communications and image employee devices to develop evidence regarding the alleged misappropriation. More than half of employees polled in a 2013 survey admitted to sending company documents to personal email addresses, 41% downloaded information to personal tablets/smart phones, and 37% sent documents to file-sharing applications such as Dropbox and Google Docs.[27] These electronic data transfers are valuable sources of evidence, and counsel should pay close attention to employee communications with third parties, documents sent to personal email accounts, and forensic evidence that the employee moved or deleted information from a company computer (or installed data-wiping programs such as CCleaner).

Key #2—Perform an Early Case Assessment

Begin with the end in mind. With litigation holds sent to custodians and potentially key evidence and discoverable data preserved, counsel in a trade secrets action should gauge the status of the litigation, where it should go, and how to get there.

As in any other case, counsel for litigants should start with the law. What is the current state of trade secrets jurisprudence? What are the risks and rewards of bringing or defending a claim? Considering the law and the evidence that has been secured, is it in the client's interests to quickly settle the matter?

Corporate defendants should—in addition to assessing possible defenses and counterclaims—consider potential claims against their *own* employees and business partners. Trade secrets lawsuits often arise in the context of an employee (or team of employees) exiting one company for another. The new employer could have claims against the new hire if the company is held liable for the employee's misappropriation of trade secrets, or if the employee made misrepresentations to the new employer regarding bringing confidential information to the company. Potential claims include contribution, indemnification (if applicable in the employment agreement), breach of contract, and fraud (misrepresentation, concealment, or deceit).

Counsel should also consider the jurisdiction in performing an early case assessment. Who is the judge and how has she ruled in similar cases? Does she commonly grant motions to dismiss? What is the composition of the potential jury pool? Will the case be tried in a county with a bevy of startup companies, a large military presence, or a significant agricultural economy?

In addition, counsel should take into account the impact of applicable procedural rules. For example, from January 1, 2012 through December 31, 2014, various counties in Colorado state courts were subject to Chief Justice Directive 11-02 and the Civil Access Pilot Project (CAPP) rules. These rules modified certain aspects of the Colorado Rules of Civil Procedure regarding "pleading, discovery, and trial management" to study reducing expenses in civil litigation and certain business actions.

On July 1, 2015, aspects of the Colorado Rules of Civil Procedure were amended in response to the pilot project. The amended rules reduce timeframes for depositions,[28] establish new guidelines for case management,[29] emphasize discovery that is proportional to the needs of the case,[30] and note that discovery should include "what a party/lawyer *needs* to prove its case, but not what a party/lawyer *wants* to know about the subject of a case."[31] These changes have significant implications for the pace, cost, and strategy of litigation and should be accounted for in an early case assessment.

A similar analysis should be performed regarding opposing counsel and their clients. Who are the attorneys and parties on the other side and what is their reputation in the community? Are they known to be aggressive or quick to settle? Have they filed similar suits in the past? If similar suits have been filed, pull those papers and analyze them; they could provide a roadmap for the current dispute.

With all the above analysis in mind, counsel should meet with clients, "communicate, communicate, communicate," and repeat. Counsel should begin an honest conversation regarding (1) the clients' goals; (2) the likelihood of litigation success; (3) the collateral consequences of litigation, including potential reputational harm and lost time dedicated to business needs; (4) expenses and budgeting for discovery, motions practice, expert witnesses, and trial; and (5) the need for buy-in from the clients and the clients' agents, including in-house counsel's (if applicable) willingness to review filings and respond to discovery requests, CRCP 30(b)(6) witnesses' willingness to speak on behalf of the company during discovery, business people's willingness to prepare for and be deposed, and a company-wide willingness to engage in disciplined document preservation.

Having this conversation early should prepare clients for what is to come from a financial and logistical standpoint, and begin what will be an ongoing process of managing emotions and expectations regarding the litigation. Business can often become personal when trade secrets are at issue. Counsel's job is to remind clients of their initial goals and keep them focused on what can realistically be accomplished through litigation and possible settlement.

Key #3—Seek or Oppose Injunctions

CUTSA allows trade secrets litigants to seek "[t]emporary and final injunctions . . . as the court deems reasonable to prevent or restrain actual or threatened misappropriation of a trade secret."[32] While permanent injunctions provide a successful plaintiff with a post-litigation remedy to prevent future use of trade secrets, temporary restraining orders and preliminary injunctions are potent tools because they can prevent a defendant from using the purported trade secrets during the course of the litigation.

Preliminary injunctions require notice to the adverse party and are intended to maintain the "status quo" while the litigation progresses through the court system.[33] A party is entitled to a preliminary injunction if it can show (1) a reasonable likelihood of success on the merits, (2) irreparable harm absent an injunction, (3) that the balance of hardships tips in its favor, and (4) that the public interest favors issuance of the injunction.[34] A temporary restraining order, on the other hand, may be granted "without written or oral notice to the adverse party" in these circumstances:

> (1) It clearly appears from specific facts shown by affidavit or by the verified complaint or by testimony that immediate and irreparable injury, loss, or damage will result to the applicant before the adverse party or his attorney can be heard in opposition, and (2) the applicant's attorney certifies to the court in writing or on the record the efforts, if any, which have been made to give the notice and the reasons supporting his claim that notice should not be required.[35]

For plaintiffs, temporary restraining orders and preliminary injunctions can be crucial. If a competitor is actively profiting from misappropriated trade secrets and potentially threatening market share, plaintiffs often cannot afford to wait until the end of the litigation for a court-ordered remedy. Conversely, for defendants, an injunction preventing the use of an alleged trade secret formula could cripple business operations.

The court could also prevent a defendant-employee from joining a new venture because the employee has knowledge of trade secrets that may be misappropriated at the new company. In *Bimbo Bakeries USA, Inc. v. Botticella*, an employer sought a preliminary injunction to prevent a former executive from working for a direct competitor.[36] The executive was one of seven employees who knew how to replicate the "nooks and crannies" texture of Thomas' English Muffins.[37] The trial court held that the employer was likely to succeed on the merits and enjoined the former executive from commencing employment with the competitor.[38]

Any court order that restricts a company's operations or the employment of an individual is a powerful tool. Temporary restraining orders and preliminary injunctions should receive particular consideration from trade secrets litigants because of their potential to provide potent remedies during the pendency of the litigation. This can place litigants in a bet-the-company posture while the case is still in its infancy.

Key #4—Identify the Trade Secrets With Particularity

Defendants in trade secrets litigation are generally entitled to "clear detail of what the plaintiff claims to be its trade secret."[39] Such disclosure is necessary and common in trade secrets litigation so that defendants can "formulate [their] panoply of defenses."[40] One Colorado court described this requirement as a prerequisite, stating that "a [p]laintiff will normally be required first to identify with *reasonable particularity* the matter which it claims constitutes a trade secret, before it will be allowed to compel discovery of its adversary's trade secrets."[41]

Defendants should take steps early in the litigation to lock their opponents into a specific and narrow definition of the alleged trade secrets. Defendants can then scrutinize the definition to determine which aspects are in the public domain, which were not kept confidentially within the company, and which otherwise do not merit trade secrets protection under CUTSA. CRCP 30(b)(6) allows parties to notice a corporate entity as a deponent and "designate with reasonable particularity the matters on which examination is requested." The organization, in turn, must designate a person to "testify as to matters known or reasonably available to the organization."[42] Defendants should take the "Rule 30(b)(6)" deposition of the plaintiff's employee with knowledge regarding the company's trade secrets, and consider taking this deposition relatively early to ensure the plaintiff's trade secrets definition is a static target throughout the pendency of the litigation.

Faced with the likelihood of a Rule 30(b)(6) deposition on this topic, plaintiffs should carefully consider who best knows *and can effectively explain* the company's trade secrets. The best witness may not be the most senior executive in the organization. In some cases, lower-level managers and/or technical employees may have the best understanding of the company's trade secrets, how they are used, and how they are protected within the organization. And just as defendants have an interest in a narrow definition of the trade secrets at issue, plaintiffs have an incentive to meet their disclosure obligations under the law with a definition that includes the broadest possible range of allegedly misappropriated information. Plaintiffs should be cautious, however, and ensure that their broad definition does not include information that is standard industry practice, available in the public domain, or otherwise not kept confidentially within the company.

Key #5—Litigate Protections for (Alleged) Trade Secrets

Despite the common posturing in a plaintiff's complaint or a defendant's motion to dismiss, discovery under the Colorado Rules of Civil Procedure—and in practically every court in the United States—eventually calls the litigants' bluff. The players take their seats. Cards are laid on the table. And the fact-finders are given the opportunity to decide who has the winning hand.

In a trade secrets case, however, the litigants' reason for being in court is predicated on a notion that their confidential, proprietary, and presumably *secret* information has been shared with the wrong people. The company that will sue to prevent its "secret sauce" from being known to or used by its competitor-defendants certainly will take umbrage with that same secret sauce being pasted on the front page of a publicly available summary judgment motion.

The Colorado Rules of Civil Procedure provide a number of provisions that litigants may use to safeguard potential trade secret information during the discovery process. Plaintiffs can move the court under CRCP 26(c) for "any order which justice requires to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense." The motion may seek limita-

tions so that (1) "the disclosure or discovery may be had only on specified terms and conditions," or (2) "a *trade secret* or other confidential research, development, or commercial information not be revealed or be revealed only in a designated way . . . ."[43] Litigants commonly furnish a proposed protective order that defines the nature of the alleged trade secret information, procedures for designating information as subject to the protective order (labeling documents "Confidential," "Highly Confidential," "Attorney Eyes Only," etc.), limitations on the use of confidential information, and who can access the information (the court, attorneys, support staff, trial consultants, etc.).

Attorney-eyes-only provisions merit particular scrutiny and consideration by plaintiffs and defendants. Depending on the language of the provision, it can restrict a document's availability to only attorneys (and their contractors), limiting client and witness access to certain information. Plaintiffs should consider these provisions because their inherent posture is to defend confidential information from those who have, on at least one occasion, allegedly sought illegal access to that information. The discovery process therefore has the potential to aid and abet a misappropriator in gaining access to *even more* trade secret data under the guise of proper discovery.

Attorney-eyes-only provisions should also be considered in circumstances in which the information in possession of the litigant is subject to a third-party confidentiality agreement. In the private equity space, for example, companies regularly share information after executing confidentiality agreements for the purpose of analyzing potential transactions. These agreements often include disclosure carve-outs for court process, but they might also require the person subject to the agreement to seek protections for the confidential information in court. To the extent that the data shared with a litigant is both discoverable and subject to a third-party confidentiality agreement, an attorney-eyes-only provision can be a useful tool to ensure compliance with litigation and contractual obligations.

Defendants should scrutinize and consider opposing attorney-eyes-only provisions because these clauses can prevent clients from assisting in the analysis of the documents and limit witnesses' ability to comment on the materials in depositions. While limitations will vary depending on the individual protective order litigated by the parties, attorney-eyes-only provisions still represent one additional—and potentially significant—barrier to a defendant's discovery process. Defendants should also consider using oppositions to any motion to protect purported trade secret information as an opportunity to attack the heart of the plaintiff's claim. Highlighting all the reasons why the information is not a trade secret calls into question the protections sought by the plaintiff and represents an additional opportunity to put the defendant's theory of the case before the judge.

Key #6—Analyze Public Access to Trade Secrets

When determining whether a plaintiff has a trade secret, litigants should consider the public availability of the contested information. Among other factors, Colorado courts consider "the extent to which the information is known outside the business" to determine whether data is worthy of trade secret protection.[44] In *I Can't Believe It's Yogurt v. Gunn*, a Colorado court refused to find misappropriation liability because the alleged trade secrets were "generally known," "readily ascertainable," and "taught at business schools."[45] Plaintiffs should seek to distinguish their information from data available in the public domain or known as a common business practice; defendants, in turn, should do the exact opposite. Defendants should break down each aspect of the purported trade secret information and identify a counterpart in the public domain.

Key #7—Deploy Policies and Procedures Strategically

For information to be trade secret under CUTSA, the owner of the data must "have taken measures to prevent the secret from becoming available to persons other than those selected by the owner to have access . . . ."[46] CUTSA simply will not presume secrecy for those who do not impose and enforce secrecy themselves. Policies and procedures regarding monitoring, labeling, and restricting access to trade secret data are all relevant to this inquiry. Counsel should also consider highlighting training programs for employees regarding keeping trade secrets confidential and any formal sanctions process for non-compliance with company protocols on this issue.

When Coca-Cola argued in a Delaware court that the formulas for its marquee beverages were trade secrets, the company detailed the extensive measures it took to maintain that secrecy, including: (1) storing the sole written versions of the formulas in a vault in Atlanta; (2) establishing a policy that only two employees may know the formulas at any given time; (3) maintaining confidentiality regarding the identities of the two employees who know the formulas; (4) allowing only the two employees who know the formulas to oversee production of Coca-Cola's secret ingredients; and (5) barring the two employees from flying on the same plane at the same time.[47]

Vaults in Atlanta and policies barring employees from traveling together are not required under CUTSA for a litigant to show it has "taken measures" to protect trade secrets. But the tangible efforts a party has (or has not) taken to safeguard its information will be subject to intense scrutiny. Litigants should prepare accordingly.

Defendants should also be ready to describe their *own* policies and procedures. Hiring protocols, joint venture protocols, employment agreements with certifications regarding third-party confidential information, due diligence on new business partners, and formal penalties for non-compliance all tell the story of a defendant working diligently to keep unauthorized information away from its business. Indeed, defendants should be able to paint the picture of a wall built with policies, procedures, due diligence, and discipline that prevents new business partners from accidentally (or intentionally) slipping past the gates with third-party trade secrets.

Key #8—Utilize Pre- and Post-Engagement Agreements

Counsel for litigants should also consider pre- and post-engagement agreements in the analysis of whether a plaintiff has taken reasonable measures to protect its alleged trade secrets under CUTSA. The existence (or absence) of confidentiality agreements, employment agreements, and non-compete agreements (including non-solicitation clauses, non-disparagement clauses, etc.) are all relevant to this inquiry. Indeed, an empirical analysis of state and federal trade secrets cases concluded that confidentiality agreements with employees or third parties were the most commonly used "measure" in cases where courts ruled that the plaintiff took reasonable steps/measures to protect its trade secrets.[48]

Confidentiality agreements and non-compete agreements assist plaintiffs by establishing the defendant-employee's awareness of confidentiality obligations. On the other hand, to the extent a plaintiff's agreements do not cover the alleged confidential information at issue, defendants should highlight the discrepancy. Defendants can also present evidence of employment agreements where incoming employees certify that they will not use third-party trade secret information at the new company.

Key #9—Strategically Use Expert Witnesses

Under CRCP 26(b)(4)(B), a litigant must show "exceptional circumstances" to discover facts known or opinions held by an expert who is not expected to be called as a witness at trial. As noted by the Colorado Supreme Court, the rule allows the attorney to "think dispassionately, reliably, and creatively both about the law and the evidence in the case and about which strategic approaches are likely to be in [her] client's best interests."[49] Litigants in a trade secrets action should take advantage of the rule to allow the non-testifying expert to educate attorneys regarding not only the nature of the purported trade secrets, but also the broader industry in which the parties operate. Counsel should query these experts regarding what is standard practice in the industry and how to define the pecuniary value of the alleged trade secrets.

In addition to utilizing paid experts, counsel should not forget about the experts they have the most access to: the clients. Trade secrets litigation regularly involves highly sophisticated business people with extensive knowledge of their industry and their company's proprietary data. While it is always a best practice to be efficient with client time and to self-educate wherever possible, counsel should not shy away from appropriate opportunities to understand the client's narrative regarding the industry and the confidential information at issue in the litigation.

Key #10—Navigate Trade Secrets Damages

CUTSA provides for (1) actual damages, (2) unjust enrichment not accounted for in the actual damages, (3) exemplary damages, and (4) in lieu of "damages measured by any other methods," a reasonable royalty for the misappropriator's disclosure or use of trade secrets.[50] Compensatory damages can be measured by methods including an "agreed value" among the parties, lost sales, lost profits, or research and development costs.[51] "Reasonable royalty" damages, on the other hand, have been described as "what the parties would have agreed to as a fair price for licensing the defendant to put the trade secret to the use the defendant intended at the time the misappropriation took place."[52]

To the extent a litigant independently brings civil theft, conversion, or unjust enrichment claims in conjunction with trade secrets claims, CUTSA can act as a barrier to recovery. The statute notably limits damages under those claims if they represent "the same operative facts which would plainly and exclusively spell out only trade secret misappropriation."[53]

Quantifying the value of a trade secret and the impact of misappropriation can be a daunting task. Courts themselves have described the measure of damages for a misappropriation case as "elusive."[54] With this consideration in mind, courts are encouraged to be "flexible" and "imaginative" in calculating these damages.[55] Litigants, in turn, should offer a roadmap the court can follow to the proper damages result (reasonable royalty, lost profits, development costs, etc.). Motions practice surrounding the initial complaint, summary judgment, and even the scope of discovery all represent opportunities for counsel to craft the damages narrative. The litigant with the least "elusive" damages theory may very well win the day.

Conclusion

While many of the strategies outlined in this article can be executed almost exclusively by an attorney, other suggestions admit-

tedly presume that companies have implemented best practices in trade secrets management before litigation is imminent, including the following: (1) establishing policies and procedures restricting access to trade secret information or deterring others from bringing third-party data to the company; (2) diligently executing confidentiality agreements with new employees and business partners; and (3) most important, thinking intentionally about what the company's trade secrets are and how that information should be protected. To the extent a company is not yet embroiled in litigation, there is no better time than the present to begin consulting counsel and developing tools that will protect future business and legal interests.

Notes

1. Ctr. for Responsible Enter. and Trade and PricewaterhouseCoopers LLP, *Economic Impact of Trade Secret Theft: A Framework for Companies to Safeguard Trade Secrets and Mitigate Potential Threats* 3 (Feb. 2014), www.pwc.com/en_US/us/forensic-services/publications/assets/economic-impact.pdf.

2. *See* Almeling *et al.*, "A Statistical Analysis of Trade Secret Litigation in Federal Courts," 45 *Gonz. L.Rev.* 291, 293 (2010) (hereinafter Almeling, "Federal Courts").

3. *See* Sanger and Perlroth, "U.S. Said to Find North Korea Ordered Cyberattack on Sony," *The New York Times* (Dec. 17, 2014), www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?_r=0.

4. Almeling, "Federal Courts," *supra* note 2 at 302–04; Almeling *et al.*, "A Statistical Analysis of Trade Secret Litigation in State Courts," 46 *Gonz. L.Rev.* 57, 68-69 (2011) (hereinafter Almeling, "State Courts").

5. Almeling, "Federal Courts," *supra* note 2 at 302; Almeling, "State Courts," *supra* note 4 at 68-69.

6. Symantec Corp., *What's Yours is Mine: How Employees are Putting Your Intellectual Property at Risk* 1 (2013), www4.symantec.com/mktginfo/whitepaper/WP_WhatsYoursIsMine-HowEmployeesarePuttingYourIntellectualPropertyatRisk_dai211501_cta69167.pdf.

7. CRS § 7-74-102(4).

8. *Colo. Supply Co., Inc. v. Stewart*, 797 P.2d 1303, 1306 (Colo.App. 1990) (quoting *Network Telecomms., Inc. v. Boor-Crepeau*, 790 P.2d 901, 903 (Colo.App. 1990)).

9. *See Tradebank Int'l Franchising Corp. v. Cmty. Connect, LLC*, No. 11-cv-01530-RPM, 2013 WL 3216113 at *2 (D.Colo. June 25, 2013).

10. *See Mgmt. Recruiters of Boulder v. Miller*, 762 P.2d 763, 765 (Colo.App. 1988).

11. *See Gold Messenger, Inc. v. McGuay*, 937 P.2d 907, 911-12 (Colo.App. 1997).

12. *Christou v. Beatport, LLC,* 849 F.Supp.2d 1055, 1074-76 (D.Colo. 2012).

13. *Coca-Cola Bottling Co. of Shreveport, Inc. v. Coca-Cola Co.*, 107 F.R.D. 288, 294 (D.Del. 1985).

14. *Data Gen. Corp. v. Digital Computer Controls, Inc.*, 357 A.2d 105, 110-11 (Del.Ch. 1975).

15. *Tan-Line Sun Studios, Inc. v. Bradley*, Civ.A. No. 84-5925, 1986 WL 3764 at *7-9 (E.D.Pa. Mar. 25, 1986).

16. *See Am. Totalisator Co. v. Auto Tote Ltd. et al.*, C.A. No. 7268, 1983 Del.Ch. LEXIS 401 at *9-11 (Del.Ch. Aug. 18, 1983).

17. *See, e.g.*, *Gillette Co. v. Williams*, 360 F. Supp. 1171, 1173 (D.Conn. 1973).

18. *Christou*, 849 F.Supp.2d at 1076.

19. *See Cellular Accessories for Less, Inc. v. Trinitas LLC*, No. CV 12-06736 DDP (SHx), 2014 WL 4627090 at *4 (C.D.Cal. Sept. 16, 2014).

20. *See PhoneDog v. Kravitz*, No. C 11-03474 MEJ, 2011 WL 5415612 at *1, *7 (N.D.Cal. Nov. 8, 2011) (denying motion to dismiss trade secrets suit seeking damages for former employee's unauthorized access to company's 17,000 Twitter followers).

21. CRS § 7-74-102(1).

22. *See* CRS § 7-74-102(2)(a).

23. CRS § 7-74-102(2)(b).

24. *Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc.*, 244 F.R.D. 614, 620 (D.Colo. 2007) (emphasis added) (citing *Zubalake v. UBS Warburg, LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003)).

25. *See Zubalake*, 220 F.R.D. at 217-18.

26. *See id.* at 219-20.

27. *See* Symantec Corp., *supra* note 6 at 1.

28. *See* CRCP 30(d)(2)(A).

29. *See* CRCP 16.

30. *See* CRCP 26(b)(1).

31. *See* Committee Comments to CRCP 26.

32. CRS § 7-74-103.

33. CRCP 65(a)(1); *Zoning Bd. of Adjustment v. DeVilbiss*, 729 P.2d 353, 357 (Colo. 1986).

34. *McData Corp. v. Brocade Commc'ns Sys., Inc.*, 233 F.Supp.2d 1315, 1319 (D.Colo. 2002).

35. CRCP 65(b).

36. *Bimbo Bakeries USA, Inc. v. Botticella*, 613 F.3d 102, 104 (3d Cir. 2010).

37. *Id.* at 105.

38. *See id.* at 108.

39. *See* Milgrim, *Milgrim on Trade Secrets* § 16.01[5][b] at 4-16 (2015).

40. *See id.*

41. *L-3 Commc'ns Corp. v. Jaxon Eng'g & Maint., Inc.*, No. 10-cv-02868-MSK-KMT, 2011 WL 10858409 at *1 (D.Colo. Oct. 12, 2011) (emphasis added; citations and quotations omitted). *See also Saturn Sys., Inc. v. Militare*, 252 P.3d 516, 522 (Colo.App. 2011) (noting that plaintiff had identified trade secrets with "sufficient particularity").

42. CRCP 30(b)(6).

43. CRCP 26(c)(2), (7) (emphasis added).

44. *See Colo. Supply Co., Inc. v. Stewart*, 797 P.2d 1303, 1306 (Colo.App. 1990) (quoting *Network Telecomms., Inc. v. Boor-Crepeau*, 790 P.2d 901, 903 (Colo.App. 1990)).

45. *I Can't Believe It's Yogurt v. Gunn*, No. Civ. A. 94-OK-2109-TL, 1997 WL 599391 at *22 (D.Colo. Apr. 15, 1997).

46. CRS § 7-74-102(4).

47. *Coca-Cola Bottling Co. of Shreveport, Inc.*, 107 F.R.D. at 294.

48. *See* Almeling, "Federal Courts," *supra* note 2 at 321-23; Almeling, "State Courts," *supra* note 4 at 80-81.

49. *See Gall ex rel. Gall v. Jamison*, 44 P.3d 233, 240 (Colo. 2002) (quoting *Intermedics, Inc. v. Ventritex, Inc.*, 139 F.R.D. 384, 392 (N.D.Cal. 1991)).

50. *See* CRS § 7-74-104.

51. *See Sonoco Prods. Co. v. Johnson*, 23 P.3d 1287, 1289 (Colo.App. 2001).

52. *See Computer Assocs. Int'l, Inc. v. Am. Fundware, Inc.*, 831 F. Supp. 1516, 1526-27 (D.Colo. 1993) (quoting *Univ. Computing Co. v. Lykes-Youngstown Corp.*, 504 F.2d 518, 530 (5th Cir. 1974)).

53. *Powell Prods., Inc. v. Marks*, 948 F. Supp. 1469, 1474 (D.Colo. 1996) (citation omitted).

54. *See Computer Assocs. Int'l*, 831 F. Supp. at 1526.

55. *Id.* ■