ACC GuideSM

Trade Secrets: Legal Framework and Best Practices for Enforcement (United States)

Sponsored by:

KILPATRICK TOWNSEND
ATTORNEYS AT LAW
Trade Secrets: Legal Framework and Best Practices for Enforcement (United States)

November 2020

Provided by the Association of Corporate Counsel
1001 G Street NW, Suite 300W
Washington, DC 20001 USA
tel +1 202.293.4103
fax +1 202.293.4107
www.acc.com

This ACC Guide provides an overview of issues that commonly arise in the United States connection with the protection and misappropriation of trade secrets. This ACC Guide aims to explain the legal framework for analysis of trade secret issues and to provide guidance in navigating the legal requirements your company might face in attempting to protect its secret information as trade secrets.

In summarizing the background legal principles underlying trade secret law, we discuss key concepts like the definitions of “trade secret” and “misappropriation” and provide examples of each, concluding with a discussion of key differences between various states’ trade secret laws. We also address the Defend Trade Secrets Act (DTSA), a recently enacted federal law that offers litigants a private cause of action in federal court for misappropriation of trade secrets. We also address some key distinctions between trade secrets and patents.

We further describe the process of categorizing, protecting, and enforcing your company's trade secret rights by identifying several "best practices" for your company to maximize the value of its trade secret portfolio and to increase the likelihood that its trade secret rights will withstand scrutiny in court. We conclude with a discussion of the evidence required to prosecute a misappropriation action, as well as the remedies available to a trade secret plaintiff.

This material was developed by Kilpatrick Townsend & Stockton LLP, the 2020 Sponsor of the ACC Intellectual Property Network. For more information about Kilpatrick Townsend, please visit www.kilpatricktownsend.com or see the “About the Authors” section of this document.

The information in this ACC Guide should not be construed as legal advice or legal opinion on specific facts, and should not be considered representative of the views of Kilpatrick Townsend & Stockton LLP or of the Association of Corporate Counsel (ACC) or any of its lawyers, unless so stated. This ACC Guide is not intended as a definitive statement on the subject, but rather to serve as a resource providing practical information to the reader.
# Contents

I. Introduction................................................................................................................................. 5

II. Background and Overview of Trade Secrets ........................................................................... 6
   A. What Constitutes a Trade Secret? ........................................................................................... 6
   B. Legal Framework of Trade Secret Protection ........................................................................ 7
   C. What Qualifies as a Protected Trade Secret? ......................................................................... 8
      1. Independent Economic Value ......................................................................................... 9
      2. Not Generally Known or Readily Ascertainable ............................................................ 10
      3. Reasonable Efforts to Maintain Secrecy ....................................................................... 11
   D. Examples of Common Types of Trade Secrets ..................................................................... 12
   E. What Constitutes Misappropriation of a Trade Secret? ........................................................ 14
   F. Just How Uniform is the UTSA? ............................................................................................ 16
   G. Distinctions Between New York Trade Secret Law and the UTSA ........................................ 16
   H. Common Scenarios in Which Trade Secrets Are Misappropriated ...................................... 17

III. Trade Secrecy under the Defend Trade Secrets Act .............................................................. 19
   A. Background of the DTSA ...................................................................................................... 20
   B. Distinctions Between the DTSA and the UTSA ................................................................. 20

IV. Trade Secrets Versus Patents .................................................................................................. 23

V. Practical Methods for Categorizing, Protecting, and Enforcing Trade Secrets ..................... 25
   A. Identifying and Categorizing Trade Secrets ....................................................................... 25
   B. Protecting Trade Secrets .................................................................................................... 26
   C. Enforcing Trade Secrets ..................................................................................................... 29
      1. Pre-Litigation Enforcement .......................................................................................... 30
      2. Litigation .................................................................................................................... 31

VI. Conclusion .............................................................................................................................. 34

VII. About the Authors .................................................................................................................. 35

VIII. Samples and Forms ............................................................................................................... 36
   A. Summary of Best Practices for Trade Secret Protection ..................................................... 36
   B. Sample Trade Secret Policy .............................................................................................. 41
C. Possible “Notice” Language About Whistleblower Immunity

D. Sample Acknowledgement Regarding Trade Secrets and Proprietary Information for Incoming Employees

E. Sample Exit Interview Form

IX. Endnotes

Copyright © 2020 Association of Corporate Counsel
I. Introduction

This ACC Guide provides an overview of issues that commonly arise in connection with the protection and misappropriation of trade secrets in the United States. This ACC Guide aims to explain the legal framework for analysis of common trade secret issues and to provide guidance in navigating the legal requirements your company might face in attempting to protect its trade secret information.

In the first section, we summarize the US background legal principles underlying trade secrecy under the three major bodies of trade secret law. In the second section, we introduce key concepts like the definitions of “trade secret” and “misappropriation” and provide examples of each, concluding with a discussion of key differences between various states’ trade secret laws. The third section discusses the Defend Trade Secrets Act (DTSA), a recently enacted federal law that offers litigants a private cause of action for misappropriation of trade secrets. The fourth section analyzes the distinctions between trade secrets and patents, presenting some considerations your company should take into account in deciding whether to protect its valuable intellectual property as a trade secret or through patent law.

In the final section, we walk through the process of categorizing, protecting, and enforcing your company’s rights in its trade secrets. This section identifies several “best practices” for your company to maximize the value of its trade secret portfolio and increase the likelihood that its trade secret rights hold up in court. We conclude with a discussion of the evidence required to prosecute a misappropriation action, as well as the remedies available to a trade secret plaintiff.

Owing to the breadth and complexity of these topics, this ACC Guide provides an illustrative, not exhaustive, treatment of the above issues. This ACC Guide primarily aims to assist in-house and outside counsel in spotting issues and addressing concerns that arise in connection with trade secret protection. The information in this ACC Guide should not be construed as legal advice or a legal opinion on specific facts, and should not be considered representative of the views of Kilpatrick Townsend & Stockton, LLP, any of its lawyers, or the ACC. This ACC Guide does not purport to constitute a definitive statement on the subject, but rather to serve as a resource providing practical information to the reader.
II. Background and Overview of Trade Secrets

Trade secret law can offer protection to valuable ideas, research, processes, inventions, and other information. Along with patents, copyrights, and trademarks, trade secrets constitute one of the four principal types of protectable intellectual property. Trade secret law applies broadly and can be more nebulous than other branches of intellectual property law, allowing protection of valuable information that, for legal or practical reasons, otherwise may not be protectable. Moreover, trade secrets may be protected simply by taking reasonable efforts to maintain their secrecy, without having to undertake a resource-intensive application or registration process. Because of the flexibility and relative ease of claiming trade secret protection, trade secrecy forms a crucial piece of the puzzle when it comes to protecting your company’s investment in research, development, or other operations that maintain its competitive edge.

This section lays out the sources of trade secret law, operative legal principles in the trade secret analysis, and the types of information that may or may not qualify as a trade secret.

A. What Constitutes a Trade Secret?

A trade secret can be virtually any information that has been kept secret and derives value by virtue of its secrecy. This broad definition embraces a wide range of intellectual property. As discussed below, secret formulas, proprietary algorithms, and innovative manufacturing processes may qualify as trade secret, but so may less obvious types of intellectual property, such as customer lists, pricing schedules, and other business information. As long as the information has value and has been kept secret, it may qualify as a trade secret.

In the United States, trade secret protection primarily derives from the common law, the Uniform Trade Secrets Act (UTSA), and the Defend Trade Secrets Act (DTSA). Although these bodies of law have important differences, all three generally agree on broad precepts such as the definitions of “trade secret,” “misappropriation,” and “improper use.” The Uniform Trade Secrets Act or a substantially similar statutory scheme has now been adopted by 49 states, leaving New York as the only state relying entirely on the common law of trade secrets. The Defend Trade Secrets Act creates a federal framework for the protection of trade secrets, allowing litigants to seek recourse in federal court without establishing diversity jurisdiction. We discuss each body of law in greater detail below.

Trade secrecy offers a number of advantages over other forms of intellectual property. Because a trade secret does not need to be registered, the holder of a trade secret can protect its information while keeping it confidential, thereby preserving its competitive advantage. Similarly, trade secrets may be relatively inexpensive to safeguard, as the holder simply needs to take reasonable efforts to maintain the secrecy of its information to enjoy trade secret protection. And trade secrecy may be available for ideas and concepts that would not be patentable because of, inter alia, the novelty and non-obviousness requirements imposed by patent law.
Between these advantages and the doctrinal stability offered by growing adoption of the UTSA, trade secret litigation has ballooned in recent decades. This increase in litigation tracks the expanding and increasingly valuable role of intellectual property as a whole in the American economy. As of 2018, intangible assets such as intellectual property comprised a record 84% of company value for S&P 500 companies, a stock market index that measures the stock performance of 500 large companies listed on stock exchange in the United States. Researchers have estimated that trade secrets represent as much as two-thirds of the value of these intangible assets. Considering these stakes, the increased investment in enforcement of trade secret rights should come as no surprise.

B. Legal Framework of Trade Secret Protection

For nearly 100 years, trade secrecy existed solely as a creature of the common law, governed by a patchwork of case law varying from state to state in the United States. Things began to change in the 1980s, following the Uniform Law Commission’s completion of the Uniform Trade Secrets Act (UTSA) in 1979, and the UTSA’s amendment in 1985. Today, 49 states have enacted the UTSA or a substantially similar statutory scheme. While there remain minor differences among some of these states, widespread adoption of the UTSA has fomented the growth of a predictable, well-established body of law. As noted above, New York constitutes the only state not to have passed the UTSA or a similar statute. But even New York may soon join the UTSA fold, as a bill had been introduced in the pandemic-interrupted 2019-20 legislative session to adopt the UTSA.

Another major shift in the legal landscape of trade secrecy came with the 2016 enactment of the Defend Trade Secrets Act, the first US federal law to create a private cause of action for misappropriation of trade secrets. Previously, litigants could not bring their misappropriation claims in federal court unless they had an independent basis for establishing federal subject-matter jurisdiction, such as complete diversity between the parties and at least $75,000 in dispute. But now, any litigant who plausibly can allege misappropriation under the DTSA may secure a federal forum for that claim. The DTSA tracks in material part the UTSA, and most federal courts apply state trade secret law to DTSA claims.

At present, a “federal common law” of trade secrets separate and distinct from state law trade secret principles has not developed. To state a claim for misappropriation under the DTSA, the subject trade secret must be used or intended for use in interstate or foreign commerce. The DTSA also can reach misappropriation that occurs outside of the United States, provided that the plaintiff establishes domestic contacts with the conduct at issue. We discuss these unique aspects of the DTSA in greater detail below.

Finally, although this ACC Guide focuses on United States’ law, international law also can provide a remedy for misappropriation of trade secrets. Most developed countries, including China, Japan, the United Kingdom, and members of the European Union, recognize and enforce trade secrecy as a form of intellectual property.
Trade secret protection varies among these jurisdictions, but generally tracks the central principles of American trade secret law. Chinese law, for example, speaks in terms of “business secrets” rather than “trade secrets,” and defines such secrets as technical or operational information not known to the public, that has commercial value, and that is the subject of measures to maintain secrecy.

International trade agreements also may guard against misappropriation of trade secret information. One such agreement, the Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement, requires countries to offer legal protection to undisclosed confidential information, which includes trade secrets or know how. According to TRIPS Article 39, the protection must apply to information that is secret, that has commercial value because it is secret, and that has been subject to reasonable steps to keep it secret. The TRIPS Agreement does not require signatories to treat undisclosed confidential information as a form of property, but does require signatories to provide an avenue for persons lawfully in control of such information to prevent its disclosure, acquisition, or use without consent in a manner contrary to honest commercial practices.

“Manner contrary to honest commercial practices” includes breach of contract, breach of confidence, inducement to breach, and the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition. The TRIPS Agreement also contains provisions on undisclosed proprietary test data and other data whose submission is required by governments as a condition of approving the marketing of pharmaceutical or agricultural chemical products which use new chemical entities. In such a situation, a TRIPS member government must protect the data against unfair commercial use. TRIPS also requires members to protect such data against disclosure, except when necessary to protect the public, or when steps are taken to ensure that the data are protected against unfair commercial use.

Similarly, bilateral investment treaties between the United States and other countries may require the foreign country to recognize certain intellectual property rights, such as trade secrecy. If your business seeks to guard against the misappropriation of trade secrets in foreign jurisdictions, you should consult an attorney licensed to practice in, and familiar with the laws of, that jurisdiction.

C. What Qualifies as a Protected Trade Secret?

Under all three bodies of American trade secret law—the UTSA, the DTSA, and the common law—establishing a protectable trade secret requires three central elements. First, the purportedly trade secret information must have independent economic value. Second, the information must not be generally known or readily ascertainable. And third, the holder of the information must take reasonable efforts to maintain its secrecy. This Subsection will outline these three elements in detail before then identifying the major distinctions between the UTSA, DTSA, and common law approaches to the definition of a protectable trade secret.
1. Independent Economic Value

Every trade secret must have some present independent economic value, whether actual or potential. Litigants frequently overlook this element. After all, if your business goes to the trouble of protecting the information (or if your competitor has undertaken to misappropriate it), then surely it must have some value. But when the occasion arises to enforce your rights in your trade secret information, failure to establish its independent economic value may bar your recovery. Two wrinkles to this element warrant additional discussion.

First, the information must be independently valuable, not just valuable to the claimant or the alleged misappropriator. In Cy Wakeman, Inc. v. Nicole Price Consulting, LLC, for example, Wakeman sought to enjoin the defendant from disseminating materials that identified Wakeman’s customers, whose identities allegedly constituted a trade secret. Wakeman claimed it derived value from the secrecy of its customers’ identities because it would not be able to generate further business if it “was unable to maintain their privacy.” The court rejected this argument, reasoning that it merely established “value to Wakeman, . . . not independent value.” Because Wakeman did not “demonstrat[e] how a competitor, armed with knowledge of Wakeman’s client relationships, could reap economic value from knowing them,” the court denied its motion for preliminary injunction.

Second, the information must be presently valuable, and not just valuable at a prior point in time. The Ohio Supreme Court’s decision in In re Review of Alternative Energy Rider illustrates this requirement. In that case, a public utilities commission determined that certain information regarding the suppliers of a utility company’s renewable energy credits, as well as the auction process for the purchase of those credits, constituted trade secrets and thus would be exempted from public disclosure. Consumer and environmental organizations appealed this determination, and the Ohio Supreme Court reversed. The Supreme Court reasoned that, even though the information had been valuable at one point, it may not have “retained its economic value in today’s market” in light of “its age and the changes in market conditions that have occurred over time.” The commission did not account for whether the information continued to carry economic value at the time of its 2013 decision, so the Alternative Energy court reversed the commission’s decision and remanded with instructions to either cite evidence establishing the present value of the information or to “publicly disclose the information that has been protected.”

These decisions illustrate common traps that befall litigants seeking to protect their allegedly trade secret information. Together they teach that, before filing suit, your business needs to prepare evidence establishing, with particularity, why your information carries present value to competitors and others in the marketplace. If you seek to protect your information as a trade secret, you should maintain evidence showing the cost of developing that information, the specific advantages your competitors might gain if they had access to the information, and the information’s utility in today’s market.
2. Not Generally Known or Readily Ascertainable

Trade secrets also must not be generally known or readily ascertainable. All three bodies of law sensibly require that, for information to be protected as a trade secret, it must actually be secret. In other words, public disclosure destroys trade secrecy, except where the trade secret consists of “a unique combination of [public] information, which adds value to the information.” The UTSA and DTSA go a step further, requiring that the information not be “readily ascertainable by proper means” by “other persons who can obtain economic value from its disclosure or use.”

Problems often arise around the “readily ascertainable” requirement when a business, through proper means, reverse engineers its competitor’s trade secrets. In MEI-GSR Holdings, LLC v. Peppermill Casinos, Inc., Peppermill accepted a $1 million fine from the Nevada Gaming Control Board for its employee’s use of a “slot machine key” to gain unauthorized access to slot machines at various casinos, including one owned by GSR. The Board’s investigation revealed that, through this unauthorized access, Peppermill had obtained the slot machines’ par values, revealing the amount of money paid out to gamblers (and the amount retained by the casino) for each machine. GSR filed suit, alleging that Peppermill misappropriated its trade secrets in violation of Nevada’s version of the UTSA. At trial, the court instructed the jury that “trade secret[s] may not be readily ascertainable by proper means, and that proper means include discovery by reverse engineering.”

The jury then returned a special verdict in Peppermill’s favor on the basis that the stolen par values could be ascertained by reverse engineering. On appeal, GSR argued that the jury instruction constituted reversible error, but the Supreme Court of Nevada affirmed. The court explained that “a defendant’s acquisition of information by proper means is a relevant consideration in determining whether the information is a trade secret,” as such proper acquisition shows that the subject information is readily ascertainable. That said, “a defendant’s acquisition of information by improper means does not preclude the defendant from demonstrating that the information is readily ascertainable by other persons.”

Problems also may arise with the “not readily ascertainable” prong when a litigant offers an overly broad definition of its trade secret information. In Farmers Edge, Inc. v. Farmobile, LLC, the court granted summary judgment in favor of the defendant on the plaintiff’s claim for violation of the DTSA. The plaintiff claimed the defendant misappropriated six trade secrets concerning strategies and plans regarding the “use of telemetrics in farming, aggregation of information, data mining, and adapting uses or applications to new and evolving technology.” But the court rejected the argument that this information constituted a trade secret. Rather, “[t]he concepts and ideas at issue were readily ascertainable through such proper means as consulting [publicly] available” standards and trade publications. The court went on to characterize the plaintiff’s alleged trade secrets as “broad, amorphous, and vague ideas” easily ascertained by knowledgeable members of the industry. Had the plaintiff better tailored its definitions of its trade secret information, it may have obtained a different result.
In sum, before claiming misappropriation under the UTSA or DTSA, consider whether your information could have been acquired by proper means—even if it actually has been misappropriated. Similarly, when defining the scope of your trade secret information, consider what sort of information may be readily ascertainable in your industry. If your definition leans too heavily on business practices or industry standards, consider whether a narrower definition would increase the likelihood that your information qualifies as trade secret.

3. Reasonable Efforts to Maintain Secrecy

Finally, information may only qualify as a trade secret if its holder has taken “reasonable” measures to maintain the secrecy of the information. As explained by retired Judge of the Court of Appeals for the Seventh Circuit Richard Posner, reasonable security of trade secret information does not require perfect security, which would stifle business and force inefficient “reconfigurations of patterns of work and production.” The efforts taken to maintain secrecy will vary from business to business in line with the business’ resources and the value of the information; thus, “reasonable steps for a two or three person shop may be different from reasonable steps for a larger company.”

First, trade secret information must be protected as to every type of authorized recipient of that information. In Broker Genius, Inc. v. Zalta, for example, the court denied a preliminary injunction on the basis that the subject information likely did not constitute a trade secret because the claimant did not impose clear confidentiality restrictions and non-disclosure obligations on its licensees. Although the claimant took employee-facing and public-facing measures to protect against disclosure of the information, its failure to do so with respect to its customers doomed its trade secret claim.

Second, trade secrets should be the subject of protective measures that exceed the protections otherwise afforded to your company’s information. In Opus Fund Services (USA) LLC v. Theorem Fund Services, LLC, the trade secret claimant argued that its use of “a password protected and restricted network” to store trade secret information, as well as a requirement that employees sign “Confidentiality Agreements prohibiting the disclosure of such information to third parties,” qualified as reasonable efforts to maintain the information’s secrecy. But the court rejected this argument, explaining that the claimant did “nothing to differentiate its protective measures for the alleged proprietary trade secrets from those imposed on any other corporate information.” Accordingly, the claimant could not establish that it had taken reasonable efforts to maintain the information’s secrecy, and the court dismissed its misappropriation claim.

Trade secret protection often hinges on the “reasonable efforts” analysis, and the case law illustrates a number of important best practices to maintain a protectable interest in your trade secrets. This ACC Guide discusses various security measures and their treatment by the courts in greater detail in Section V below.
D. Examples of Common Types of Trade Secrets

Customer Lists and Databases. Companies frequently claim trade secret protection for customer lists and databases, which generally can constitute a trade secret if the holder can demonstrate the list is not readily ascertainable and has been kept confidential. But one court found a customer list based largely on the membership of a trade association did not constitute a trade secret, because “a person could readily ascertain a vast majority of [the] customer list from [the trade association’s] publications and could contact those customers in an effort to solicit their business.”

Similarly, trial courts have held that failure to properly safeguard a customer list will preclude trade secret protection. In M.J. McPherson Services, LLP v. Sports Images, Inc., McPherson provided the defendant with a list of McPherson’s customers, to whom the defendant agreed to ship trading cards. When the defendant later began contacting McPherson’s customers to sell them trading cards directly, McPherson sued, claiming misappropriation of its allegedly secret customer list. The court held that McPherson failed to state a claim for misappropriation, reasoning that McPherson “fail[ed] to allege it took precautions to prevent Defendant from using the customer list for business outside of the agreement; that the agreement contained a non-disclosure or confidentiality clause; or that it communicated to Defendant that it believed the customer list to be a trade secret.” Accordingly, the customer list did not constitute a trade secret.

Business Strategies and Ideas. Business strategies and ideas can also constitute trade secrets, so long as the trade secret claimant is able to describe a sufficiently concrete idea and otherwise establish the elements of trade secrecy. In GlobalTap LLC v. Elkay Manufacturing Co., the Northern District of Illinois held that GlobalTap’s business plan did not warrant trade secret protection. GlobalTap sought protection for an entire 101-page business plan, which included generally available statistics on “global water issues” and a global survey of regulations for bottled water. The court held that the business plan reflected “general areas of information,” and that, while “[t]here may well be trade secrets within the 101-page business plan,” GlobalTap failed to identify them with specificity. As a result, the business plan did not constitute a trade secret. By contrast, the plaintiff in Engility Corp. v. Daniels specifically identified the “internal pricing and competition strategies” within the confidential documents misappropriated by the defendant, so the District of Colorado had little problem finding that the valuable, confidential information qualified as a protected trade secret.

Software. Software also may qualify as a trade secret, but issues often arise when the software has been provided to third parties and not just used internally. Such cases often turn on whether the software’s creator took reasonable steps to maintain the confidentiality of its source code and whether the software license agreements include confidentiality and non-disclosure restrictions.
In *GlobeRanger Corp. v. Software AG U.S.A., Inc.*, for example, the US Court of Appeals for the Fifth Circuit affirmed a jury verdict awarding GlobeRanger $15 million for the misappropriation of its trade secret software. Among other safeguards, GlobeRanger entered into licensing agreements with third parties to limit their use of its software, requiring the use of a “unique license key” to access the software, which allowed GlobeRanger to “limit use of the product for a certain time period or to a certain number of devices.” GlobeRanger also kept its source code under lock and key, “restricting access to [its] data center; requiring double password protection to access the ‘source code control system’; [and] limiting access to source code only to developers rather than all employees.”

As long as your company only discloses its software to third parties under licenses or other agreements requiring confidentiality, the software may retain trade secret status notwithstanding the number of licensees. In other words, even if your company licenses its software to thousands of end users, the software still may qualify as a trade secret if the subject license agreements require licensees to keep the software confidential. Of course, if your company sells its software publicly, rather than licensing it under an agreement requiring confidentiality, the software may lose its trade secret protection.

**Data Compilations.** In addition, data compilations may receive trade secret protection even if comprised of information in the public domain, so long as the compilation combines the public information in a unique manner that is both secret and valuable. In *AirFacts, Inc. v. de Amezaga*, for instance, AirFacts claimed that a former employee violated the Maryland enactment of the UTSA by misappropriating certain flowcharts. The flowcharts reflected airfare price rules and processing information compiled from a private database accessible to any subscriber, organized in a certain manner to allow “more systematic and easier” audits of ticket prices. The district court held the flowcharts did not constitute trade secrets “because they [we]re simply an ‘overview’ of publicly available . . . information that AirFacts did not own,” but the US Court of Appeals for the Fourth Circuit reversed. The appellate court reasoned that the “painstaking, expert arrangement of the [publicly available] data made the Flowcharts inherently valuable separately and apart from the publicly available contents,” such that they could qualify as trade secrets despite being comprised entirely of non-confidential information. Because AirFacts took reasonable measures to maintain the flowcharts’ secrecy, they qualified as protected trade secrets.

Finally, not all confidential information qualifies as trade secret. This problem commonly arises where the holder of information takes steps to maintain its confidentiality, but the information has no independent economic value. This might result from the information’s lack of value in the first place, or from formerly valuable information losing its value over time. Price lists, for example, lose economic value as the marketplace changes, and will not retain trade secret protection even if kept confidential. When confidential but non-trade secret information has been misappropriated, other common law doctrines such as conversion or breach of a confidentiality agreement may provide a remedy.
E. What Constitutes Misappropriation of a Trade Secret?

The holder of a trade secret has the right to prevent or seek damages for misappropriation of its trade secrets. As defined by the UTSA, misappropriation occurs where a person acquires, uses, or discloses trade secret information acquired by improper means or in breach of a duty of confidentiality.93 Under both the UTSA and DTSA, “improper means” refers to conduct that fails to meet reasonable standards of business ethics and commercial morality, such as bribery, theft, misrepresentation, or espionage.94

As illustrated by a pre-UTSA decision, *E.I. DuPont de Nemours & Co. v. Christopher*, dishonest but technically legal conduct can still qualify as “improper means.”95 In that case, DuPont had developed a proprietary method to produce methanol for a price lower than its competition. As DuPont began construction of a plant dedicated to the novel manufacturing process, an unknown third party hired a pilot to fly over the plant’s build site and photograph the then-visible methanol production line. DuPont alleged that its trade secret production process could be deduced from such aerial photographs. The US Court of Appeals for the Fifth Circuit held DuPont’s allegations stated a claim for misappropriation of trade secrets.96 The court explained that, although the photographers did not trespass on DuPont’s property, breach a confidential relationship, or take other illegal acts, DuPont’s allegations established that the photographers had acquired its trade secrets through improper means.97

A duty of confidentiality may flow from one of several sources. The duty most frequently arises by contract, such as where an employee signs a confidentiality agreement as a condition of employment.98 A duty of confidentiality also may be implied where the recipient of the information knew or should have known that the information was intended to be kept confidential, and the provider of the information could reasonably infer that the recipient consented to keep the information confidential.99 Courts have implied such a duty between employees and employers,100 between parties to commercial transactions,101 and in other situations where a reasonable person would understand the information it had received had been provided on a confidential basis.102

The US Uniform Trade Secrets Act (UTSA) also imposes a knowledge requirement, under which the holder of the trade secret must prove that the user or acquirer of trade secret information knew or should have known that the information had been acquired by improper means or in breach of a duty of confidentiality. Constructive knowledge may arise where the improper means would be obvious to a reasonable acquirer of the information.103 In *Experian Information Solutions, Inc. v. Nationwide Marketing Services, Inc.*, the defendant acquired a data compilation from a third party that the plaintiff alleged had been stolen from its records. The court held that, because the defendant “paid less than 1% of the market rate for a one-time license” for the data, and because the defendant was able to purchase the data outright (rather than licensing it, consistent with the usual practice in the industry), the defendant should have known that the information it had acquired constituted a trade secret obtained through improper means.104
Misappropriation gives rise to a number of remedies, including damages, injunctive relief, and (sometimes) attorneys’ fees, as discussed in greater detail in Section V.C.2. below. For purposes of this overview, **compensatory damages** include: (i) the actual loss caused by the misappropriation, generally measured by the holder’s lost profits; (ii) the unjust enrichment of the misappropriating party, which may be awarded instead of or in addition to lost profits; or (iii) a reasonable royalty for the use of the misappropriated trade secret, which may be awarded where damages cannot easily be measured by the other methods.\(^{105}\) **Exemplary or punitive damages** also may be available in cases of “willful and malicious misappropriation,”\(^ {106}\) and **injunctive relief** may be obtained to enjoin actual or threatened misappropriation.\(^ {107}\) The ability to enjoin threatened disclosure has led to the creation of a “de facto noncompete” under the inevitable disclosure doctrine (discussed in greater detail below) which may temporarily prevent employees from working for competitors of their former employers.\(^ {108}\)

**Finally, the statute of limitations for a misappropriation claim runs for three years, beginning on the date the misappropriation was discovered or should have been discovered by reasonable diligence.**\(^ {109}\)** In applying the discovery rule, courts have held the UTSA requires something more than “mere suspicion of possible misappropriation,”\(^ {110}\) but less than “knowledge of every fact necessary to prevail on the [misappropriation] claim.”\(^ {111}\) *Porex Corp. v. Haldopoulos* illustrates the degree of knowledge necessary for the limitations period to begin to run.\(^ {112}\) In that case, Porex sent a letter to its former employee in April 2000, claiming it had “strong reason to believe that Mr. Haldopoulos has misappropriated and is continuing to misappropriate Porex’s trade secrets and confidential information.”\(^ {113}\) Porex did not file suit until September 2005, and Haldopoulos moved for summary judgment claiming that Porex’s claim was time-barred.\(^ {114}\) The trial court granted summary judgment, but the Court of Appeals reversed, looking past Porex’s fears and suspicions and instead relying on the “objective information” known to Porex in the spring of 2000.\(^ {115}\) At that time, Porex only knew “that within a few months of leaving the company’s employ, Haldopoulos was manufacturing plastics out of a facility owned by one of its former customers and had hired another former Porex employee to assist him.”\(^ {116}\) Because Porex had not “identified any particular confidential information that it believed Haldopoulos was using,” an issue of fact existed regarding “whether the suspicions reflected in [the] letter were sufficient to cause a reasonably prudent person to investigate whether its trade secrets had been misappropriated.”\(^ {117}\) Accordingly, the appellate court reversed the trial court’s grant of summary judgment.\(^ {118}\)

Conversely, if the holder of a trade secret uncovers facts suggesting that specific information has been misappropriated, **the discovery rule will toll (i.e., pause) the limitations period only if the holder Investigates the suspected misappropriation.**\(^ {119}\)** In *Harry Miller Corp. v. Mancuso Chemicals Ltd.*, two major purchasers of Miller’s trade secret acid inhibitor took their business elsewhere in 1991.\(^ {120}\) By August 1991, Miller “developed suspicions that [a former employee] had stolen the formula for [Miller’s acid inhibitor]” and was selling a knock-off inhibitor to Miller’s former customers.\(^ {121}\) Miller, however, “conducted no serious investigation into the origins of [the knock-off inhibitor], and never sought the help of anyone to resolve its uncertainty” regarding the knock-off’s provenance.\(^ {122}\)
Miller eventually filed suit in 1999, after testimony in another action revealed the origin of the knock-off. The trial court granted summary judgment in favor of the defendant on Miller’s misappropriation claim, reasoning that the discovery rule did not apply due to Miller’s “dilatory and disinterested approach to protecting its rights.” The court further rejected Miller’s argument that it “could not confirm the source of [the knock-off] product,” explaining that “[a]n injured party faced with uncertainty must make some effort to discover facts relating to his injury before he gives up his investigation.”

F. Just How Uniform Is the UTSA?

Despite near-universal adoption of the UTSA, small differences abound among state enactments of the uniform act. Most of these differences are minor: for instance, the Texas version of the UTSA adds “financial data” and “list[s] of actual or potential customers or suppliers” to the specified types of information that may qualify as trade secret. Three recurring points of distinction, however, merit some additional discussion.

First, not every US state utilizes the three-year statute of limitations set by the UTSA. The statute varies from two years in Alabama to five years in states like Illinois and Georgia. Second, as discussed more thoroughly in Section V.C.2, below, different jurisdictions impose different pleading requirements for a misappropriation claim to survive a motion to dismiss. In California, trade secrets must be identified with “reasonable particularity” before discovery commences, while Kentucky law only requires a litigant to identify “general categories of its trade secrets” that allegedly have been misappropriated. And third, states vary significantly on the amount of, and burden of proof for, exemplary or punitive damages, with some states disallowing them altogether, others allowing them up to a certain amount, and still others allowing an unlimited amount of exemplary damages. Careful practitioners should look for these and other differences before litigating in an unfamiliar jurisdiction.

G. Distinctions Between New York Trade Secret Law and the UTSA

Although the UTSA generally tracks common law principles, a handful of distinctions merit special attention. New York, the sole remaining “common law” jurisdiction, defines a trade secret as “any formula, pattern, device or compilation of information which is used in one’s business, and which gives one an opportunity to obtain an advantage over competitors who do not know or use it.” Drawing from the Restatement (First) of Torts, published in 1939, New York courts consult six factors to determine whether information qualifies as a trade secret, with no single factor being dispositive. This approach gives a broader definition to trade secrecy than the UTSA in some respects, but a narrower one in others.

Unlike the UTSA, New York courts consider the expense incurred in developing the trade secret. This means that, while the UTSA may protect trade secrets developed accidentally or for a low cost, such information may not be protectable under New York law.
In the same vein, New York limits trade secrecy to “process[es] or device[s] for continuous use in the operation of the business,” as opposed to “information as to single or ephemeral events in the conduct of business.” The UTSA does not impose a similar requirement. Thus, as illustrated by one commentator, the UTSA would protect the formulas for both Coca-Cola® and New Coke™, but New York law only would protect the formula for Coca-Cola®, because Coca-Cola no longer uses New Coke™ in its business. This “continuous use” requirement precludes protection of so-called “negative know-how,” such as failed prototypes or “blind alleys” during research and development.

Conversely, New York law does not explicitly require that the holder of the trade secret take reasonable measures to protect its information. But this appears to be a distinction without a difference, as various factors considered by New York courts pertain to the measures taken to safeguard the secrecy of the information.

New York law also differs from the UTSA in terms of available remedies. As discussed in Section V.C.2, below, New York courts do not award unjust enrichment damages based on the defendant’s avoided development costs. Similarly, while the UTSA provides for injunctive relief in cases of threatened misappropriation, New York law requires litigants to make the traditional four-element showing for injunctive relief, including a likelihood of success on the merits. By extension, New York courts generally reject the inevitable disclosure doctrine “absent evidence of actual misappropriation by an employee.” Along the same lines, while the UTSA authorizes an award of attorneys’ fees to the prevailing party in cases of bad faith, New York law only grants prevailing parties their attorneys’ fees where the opposing party acted maliciously and was “entirely motivated by a disinterested malevolence.” Claimants may be unable to make this showing in the trade-secret context, as the misappropriation will almost always be motivated by the profits to be derived from the trade secret, and not just an intent to harm the plaintiff.

H. Common Scenarios in Which Trade Secrets Are Misappropriated

Recurring fact patterns in the US case law illustrate common situations involving trade secrets misappropriation.

First, departing employees frequently find themselves facing trade secret misappropriation suits, a pattern than has been exacerbated with rising employee mobility. In *National Fish & Seafood, Inc. v. Scanlon*, for example, the Director of Research and Development and Quality Assurance for National Fish accepted a job offer from a competitor. Before she gave notice to National Fish, she copied “literally thousands of documents” onto a USB drive, including “recipes, cost analyses, policy documents, current and former product specifications, and a slew of documents regarding . . . a major National Fish customer.” National Fish sued, claiming the departing employee had misappropriated its trade secrets, and sought a preliminary injunction to prevent disclosure or use of the trade secrets. The court granted the requested injunction, enjoining the former employee from viewing the misappropriated documents or using the information they contained. The court further enjoined the defendant from beginning her employment at National Fish’s competitor pending the final adjudication of National Fish’s claims.
Misappropriation claims also may be available absent the sort of blatant theft in *National Fish*. In *Cerro Fabricated Products LLC v. Solanick*, Cerro’s former president left to join a competitor after working for Cerro for six years. During the president’s tenure with Cerro, he dealt with trade secret information regarding Cerro’s pricing, profit margins, manufacturing processes, and marketing, strategic, and business plans. Although Cerro presented “no direct evidence” the former president even attempted to disclose these trade secrets to his new employer, the court concluded he likely possessed “a significant amount of confidential information, including certain trade secrets, about Cerro in his memory.” Remarking on the fact the competitor did not present “any evidence of any steps that [the former president] or [the competitor] have taken or intend on taking in order to prevent the disclosure of any of Cerro’s trade secrets or confidential information,” the court enjoined the former president “from revealing Cerro’s trade secrets.” The court declined to enjoin the former president from working for Cerro’s competitor, however, reasoning that the public interest and the risk of harm to both the former president and the competitor “weigh[ed] against any injunctive relief barring [the former president] from working for any period of time.”

Second, trade secrets may be misappropriated in connection with licensing and other business relationships with third parties. As illustrated by *Liqwd Inc. v. L’Oreal USA Inc.*, your company should be wary of sharing its trade secret information with third party businesses without adequate protection. In that case, a start-up company, Olaplex, entered into acquisition discussions with “established industry stalwart” L’Oreal. After executing an non-disclosure agreement (NDA) with L’Oreal, Olaplex shared trade secret and confidential information regarding its testing of proprietary hair treatment technology. After receiving the information, L’Oreal declined to acquire Olaplex. Instead, it allegedly used the trade secrets to accelerate development of a competing line of hair treatment products, which L’Oreal took to market less than one year after the parties’ initial meeting. Olaplex filed suit in the District of Delaware in January 2017, alleging that L’Oreal had misappropriated its trade secrets under both the DTSA and the Delaware version of the UTSA. In August 2019, following a week-long trial, the jury found that L’Oreal had misappropriated Olaplex’s trade secrets, awarding damages to Olaplex in the amount of $22,265,000.

While *L’Oreal* illustrates the need for confidentiality agreements when dealing with third parties, *Alta Devices, Inc. v. LG Electronics, Inc.* highlights the importance of those agreements’ duration and expiration dates. In that case, Alta entered into discussions with LG in 2011 and 2012 regarding a potential investment in Alta or other business opportunities related to a novel solar film technology developed by Alta. Alta shared its technology with LG under an NDA, but LG declined to make its proposed investment. LG then approached Alta as a potential customer in 2013 and 2014 and received a sample of the solar film material. But rather than purchasing Alta’s product, LG allegedly used the information and material shared by Alta to reverse engineer the solar film, as discovered by Alta in 2016 when LG began producing publications describing similar solar cell structures and applying for patents that appeared to incorporate aspects similar to Alta’s production process.
Alta demanded that LG return the information and material, as required by the NDA, but LG only returned some of the documents and two of the five samples. Alta then sued for misappropriation of its trade secrets under the DTSA and the California version of the UTSA, and LG moved to dismiss. LG argued that the NDA expired in 2015, so Alta’s information lost its trade secret protection once LG no longer had an obligation to maintain its confidentiality. But the court rejected this argument, holding that the NDA was ambiguous as to its expiration date, such that resolution of the claim on a 12(b)(6) motion would be inappropriate. This decision illustrates that, if your NDAs or other confidentiality agreements have an expiration date, those agreements should provide that trade secrets maintain their confidentiality as long as the trade secret information remains a trade secret, notwithstanding the expiration of the confidentiality obligation with respect to non-trade secret information.

Third, recent years have seen a rise in cyber theft and economic espionage. As of 2015, trade secret theft through cyber espionage cost the United States economy as much as $180 billion. In part, this reflects the relative ease of stealing intellectual property during the digital age. Before computers became ubiquitous, a would-be thief could only get his or her hands-on confidential materials after accessing a secure facility, furtively copying the information, and sneaking out physical copies. But today, hundreds of thousands of documents can be downloaded to a USB drive small enough to fit on a keychain, or accessed electronically by a hacker on the other side of the world. In the same vein, misappropriation by foreign actors has increased markedly in recent years, with some nations actively encouraging economic espionage to kickstart or supplement domestic growth and innovation.

III. Trade Secrecy under the Defend Trade Secrets Act

Because the US Congress modeled the Defend Trade Secrets Act (DTSA) on the Uniform Trade Secrets Act (UTSA), the two bodies of law largely converge around the same principles. Certain unique aspects of the DTSA, however, merit independent discussion. The DTSA provides a basis for federal question jurisdiction, granting access to the federal courts that litigants otherwise may not enjoy. Similarly, the DTSA reaches certain extraterritorial conduct and authorizes ex parte seizures to prevent the use or disclosure of misappropriated trade secret information. This Section discusses these and other aspects of the DTSA, before delving into the recent developments and other changes in the trade-secret landscape caused by the DTSA’s enactment.
A. Background of the DTSA

Enacted in 2016, the DTSA represents the first federal law to create a private cause of action for the misappropriation of trade secrets. The DTSA largely mirrors the UTSA in structure and substance. Both bodies of law utilize identical or substantially similar definitions for “trade secret,” “misappropriation,” and “improper use.” The DTSA also measures monetary damages in the same manner as the UTSA, with claimants entitled to damages for their actual loss plus any unjust enrichment received by the defendant, or a reasonable royalty for the unauthorized use of the trade secret. (Note, however, that fees appear to be awarded more frequently, to both plaintiffs and defendants, under the DTSA.) Both acts also impose a three-year statute of limitations. As a result, courts applying the DTSA frequently draw from UTSA case law, leading to a federal scheme that complements, rather than displaces, state law.

B. Distinctions Between the DTSA and the UTSA

Despite these similarities, the DTSA and the UTSA differ in several respects:

- First, the DTSA’s reach differs from that of the UTSA, and certain conduct actionable under one act does not give rise to a cause of action under the other.
- Second, the DTSA expressly provides for ex parte seizures to protect against misappropriation. And third, the DTSA exempts whistleblowers from liability and requires employers to provide notice of the exemption in any contract governing the use of confidential information.

Most of the differences in the breadth of the UTSA and DTSA flow from the DTSA’s character as a federal statute only recently signed into law. The DTSA carries an effective date of May 11, 2016, and only applies “to misappropriations that occur or continue to occur on or after” that date. Continued possession of a trade secret after the effective date, without additional instances of unauthorized acquisition, use, or disclosure, does not suffice to bring misappropriation under the purview of the DTSA. Similarly, because the DTSA’s enactment reflects an exercise of Congress’s commerce power, the act only reaches misappropriation of trade secrets “related to a product or service used in or intended for use in interstate or foreign commerce.” If a trade secret claimant can make these showings, it can establish subject-matter jurisdiction in federal court. Some federal courts have concluded, however, that failure to plead a nexus with interstate commerce warrants dismissal of a DTSA claim.

Unlike the UTSA, the DTSA provides for extraterritorial application. Specifically, the statute “applies to conduct occurring outside the United States” if (1) the offender is an American citizen, permanent resident, or an entity organized under American law; or (2) if “an act in furtherance of the offense was committed in the United States.” In a recent, well-reasoned decision, the Northern District of Illinois shed light on the otherwise murky reach of subsection (2).
Drawing on case law interpreting “in furtherance of” language in other statutes, the court reasoned that Section 1837 will be satisfied if some domestic conduct “manifest[s] that the [misappropriation] is at work.” Because the defendants in that case had “advertised, promoted, and marketed products embodying the allegedly stolen trade secrets domestically at numerous [domestic] trade shows,” they had committed acts in furtherance of the trade secrets’ use (and, by extension, misappropriation) within the United States. Accordingly, the court allowed plaintiffs to introduce evidence at trial of damages suffered outside of the United States because of the alleged misappropriation.

The plain language of the DTSA also appears to limit application of the inevitable disclosure doctrine. This doctrine, rooted in the UTSA’s prohibition of “threatened misappropriation,” allows courts to prevent an employee from working (at least temporarily) for a new employer when that employee had access to the former employer’s trade secrets and the proposed new responsibilities make it “inevitable” that he or she would use or disclose those trade secrets in performing the new job’s responsibilities.

In the leading case on the inevitable disclosure doctrine, *PepsiCo, Inc. v. Redmond*, the Seventh Circuit affirmed a preliminary injunction prohibiting a PepsiCo executive from accepting a position with Quaker Oats, PepsiCo’s then-competitor in the market for sports drinks. The court reasoned that the executive “cannot help but rely on [PepsiCo’s] trade secrets as he helps plot Gatorade’s and Snapple’s new course, and . . . these secrets will enable Quaker to achieve a substantial advantage by knowing exactly how [PepsiCo] will price, distribute, and market its sports drinks and new age drinks and being able to respond strategically.” Consequently, even though PepsiCo adduced no proof of actual misappropriation, the Seventh Circuit held that the district court properly enjoined the executive from working for Quaker for six months.

Despite the inclusion in the DTSA of language apparently aimed at curbing application of the inevitable disclosure doctrine, courts generally have continued to apply the doctrine in line with state law. The DTSA prohibits injunctions that “prevent a person from entering into an employment relationship” unless the injunction is “based on evidence of threatened misappropriation and not merely on the information the person knows.” In theory, this language prevents broad application of the inevitable disclosure doctrine. But in practice, some courts continue to apply prior law regarding that doctrine. In *Fresco Systems USA, Inc. v. Hawkins*, for example, US Court of Appeals for the Third Circuit affirmed a district court’s finding that irreparable harm would result if a former employee had not been enjoined from working for a competitor. In so doing, the court accepted the district court’s conclusion that, even absent specific evidence of threatened misappropriation, an injunction properly issued because the ex-employee “would likely use his confidential knowledge to [his former employer’s] detriment.”

Conversely, in *UCAR Technology (USA) Inc. v. Yan Li*, the US District Court for the Northern District of California rejected an inevitable-disclosure theory of misappropriation liability and ordered that allegations supporting that theory be stricken from the plaintiff’s complaint. The court based its holding on case law interpreting the California version of the UTSA, reasoning that “California courts have resoundingly rejected claims based on the ‘inevitable disclosure’ theory.” Thus, the DTSA seems unlikely to change the existing split across jurisdictions as to the inevitable disclosure doctrine.
The DTSA also provides a powerful remedy for misappropriation in the form of its *ex parte* seizure provision. Under that provision, a court may enter an *ex parte* order “providing for the seizure of property necessary to prevent the propagation or dissemination of the trade secret” if the movant demonstrates “extraordinary circumstances,” including that “the person against whom seizure would be ordered . . . would destroy, move, hide, or otherwise make [the] matter [to be seized] inaccessible to the court, if the applicant were to proceed on notice to such person.” The US District Court for the Northern District of Indiana has interpreted the statutory language as authorizing application of the seizure provision even where “seizure could not be accomplished by way of Rule 65.” And other courts have not hesitated to grant *ex parte* temporary restraining orders under Rule 65 that accomplish the same ends as the seizure provision. But some courts have declined to order *ex parte* seizures, only to enter Temporary Restraining Orders (TROs) enjoining access or modification of the subject information and requiring that the information be delivered to the court for a hearing on a preliminary injunction. Practitioners should pay attention to this rapidly developing area of law as courts continue to interpret the DTSA.

Finally, the DTSA provides immunity for whistleblowers who disclose trade secrets to attorneys or government officials “solely for the purpose of reporting or investigating a suspected violation of law.” Thus far, courts have provided little guidance on this provision. In one early decision, *Unum Group v. Loftus*, the US District Court for the District of Massachusetts denied an alleged whistleblower’s motion to dismiss the DTSA claim alleged against him, reasoning that no facts in the record “support[ed] or reject[ed] his affirmative defense at this stage of litigation,” and relying on the fact that the whistleblower “ha[d] not filed any potential lawsuit that could be supported by information in those [allegedly misappropriated] documents.” Conversely, the US District Court for the Eastern District of Pennsylvania has dismissed a DTSA claim on the basis of Section 1833, where an ex-employee disclosed alleged trade secrets to her attorney in connection with a lawsuit against her former employer for violations of Title VII and the Americans with Disabilities Act of 1990 (ADA). As with the seizure provision, this facet of the DTSA continues to evolve as more courts confront the whistleblower immunity provision.

The DTSA also requires that employers provide notice of whistleblower immunity “in any contract or agreement with an employee that governs the use of a trade secret or other confidential information.” This requirement also may be satisfied by “a cross-reference to a policy document provided to the employee that sets forth the employer’s reporting policy for a suspected violation of law.” If the employer fails to provide such a notice to an employee against whom the employer has brought a DTSA claim, the employer is barred from recovering exemplary damages or attorneys’ fees. A sample notice form is attached in the Appendix.
IV. Trade Secrets Versus Patents

Trade secret law and patent law reflect distinct but complementary approaches to the protection of similar types of intellectual property. Frequently, the same item of information may be patented or protected as a trade secret, leaving businesses with a difficult decision regarding how to protect their intellectual property. Moreover, because the publication of a patent application destroys the confidentiality required for trade secrecy, patents and trade secrets generally constitute mutually exclusive options. But in the hands of a skilled practitioner, trade secrecy and patent law can work together to provide more complete protection of your company’s intellectual property. This Section analyzes the relative benefits of each body of law before suggesting a combined approach to the use of trade secret and patent protections to ensure the broadest possible protection of your company’s intellectual property.

Trade secrecy has a number of advantages over patent law. Certain information not entitled to patent protection may still qualify as trade secret. Patents only may be issued to protect inventions that satisfy relatively rigorous requirements of usefulness, novelty, and non-obviousness “to a person having ordinary skill in the art to which the claimed invention pertains.” No such obligations apply to trade secrets, which can consist of mere combinations of publicly available data.

Similarly, trade secrecy may be able to protect so-called “negative know-how,” such as dead ends in research and development, or early ideas that, if disclosed, could provide a competitor with a jump-start in its own development efforts. As Thomas Edison famously said after testing and rejecting ten thousand prototype lightbulbs: “I have not failed 10,000 times. I have not failed once. I have succeeded in proving that those 10,000 ways will not work.” Those rejected prototypes could receive trade secret protection, even though none were commercially viable (and hence lacked the utility required by patent law). As a more recent example, the US District Court for the District of Delaware has granted trade secret protection to negative know-how regarding failed designs for self-retracting vacuum hoses. In short, intangible assets that serve to avoid failure can be at least as valuable as knowledge that enables success. Thus, the breadth and flexibility of trade secrecy gives it certain inherent advantages over patent law.

Trade secrecy also may be preferred over patenting an invention because of the costs, delays, and other burdens of the patent application process. Trade secret protection automatically attaches to information that meets the definition of a trade secret, a far cry from the patent application process, which may entail a delay of months or years between the initial application and the issuance of a patent. Trade secrets may (and indeed must) be kept confidential, in contrast with the risk of a competitor scrutinizing your company’s rejected patent applications to copy intellectual property that may not be patentable. Similarly, the up-front cost of trade secret protection appears minimal compared to the costs of preparing a patent application; all the holder of the information must do is take reasonable measures to maintain its confidentiality. Finally, trade secret protection may be indefinite in duration.
For example, the Coca Cola® formula remains a protected trade secret more than 100 years after its invention. Patent rights, on the other hand, expire at the end of the patent term, and can be lost earlier if maintenance fees have not been paid. Trade secrets therefore may be preferable because they allow holders of information to avoid the burdens and risks attendant to the patent application process.

Of course, patents have several distinct advantages over trade secrets. As discussed above, trade secret protection may be difficult to achieve in many contexts. If the information you seek to protect will be disclosed or readily ascertainable in its commercial use, patent protection likely will be superior to trade secrecy. Patent law offers better protection to technology contained in consumer products, such as the click wheel used in the iPod Classic™. Patents also grant exclusivity, prohibiting infringement even where a competitor independently develops or reverse engineers your patented technology. In contrast, information that may be reverse engineered generally qualifies as "readily ascertainable," and therefore cannot receive trade secret protection.

Thus, in circumstances where your business has such a research lead on its competitors that it faces only a minimal risk of reverse engineering, trade secrecy may be the way to go. But if your business has only narrowly edged out its competitors in a rush to bring new technology to market, patent law likely provides the best protection to your business’s intellectual property.

In some situations, the unique benefits of trade secret and patent protections can be combined through savvy use of both of these branches of intellectual property. In drafting patent applications, certain aspects of your business’s proprietary information inevitably will be left on the patent “cutting room floor.” Trade secrecy may be well suited to protect this penumbra of valuable, but not patentable, information. Indeed, in contrast to the patentable information that rises up from the patent cutting room floor, reasonable confidentiality measures may be all that is required to assert trade secret protection for the unpatentable information; given the likely value of the information, it may be worthwhile to take steps to assert such protection. To borrow an example from the US District Court for the District of Delaware, the successful design of a retractable vacuum hose could be the subject of a patent application, while the negative know-how regarding the failed designs may be protected as trade secrets. By taking such a holistic approach, your business can draw concentric circles of protection around its innovations. Patentable information sits in the inner ring, protected by patent law; non-patentable trade secrets sit in the middle ring, protected by trade secrecy; and non-trade secret confidential information sits in the outer ring, protected by confidentiality agreements and common-law property and tort doctrines.
V. Practical Methods for Categorizing, Protecting, and Enforcing Trade Secrets

As discussed above, trade secrecy can play a key role in the protection of your business’s valuable intellectual property. Because of the breadth and flexibility of trade secret law, employing a handful of best practices can allow your business to maximize the benefits it receives from the trade secrecy of its information. This Section analyzes such practices, starting with the initial identification and classification of trade secrets, then turning to the protective measures required to establish trade secrecy, and finishing with how to best position your business to enforce its trade secrets before and during litigation.

A. Identifying and Categorizing Trade Secrets

To protect your business’s trade secrets, you first must identify and classify any information that may be subject to trade secret protection. Many businesses successfully manage such internal classification regimes by creating an Intellectual Property (IP) committee to oversee the firm’s portfolio of intellectual property. This tried and true method can help ensure that, if and when a threat arises to your business’s intellectual property, you will be prepared to take swift, effective protective action.

Although an IP committee may be more familiar to technology companies or other entities with a primary focus on intellectual property, an IP committee can help companies of all stripes preserve the value of their holdings. To best advance this goal, the IP committee should be comprised of representatives with expertise in at least six fields:

- a technical representative, who can speak to the technologies and information developed by your company;
- a marketing representative, who can speak to the demand for such technology or information in the marketplace;
- a strategic representative, who can speak to how the subject technology or information fits in the company’s strategic plan, as well as the anticipated business plans of its competitors;
- a financial representative, who can speak to the economic costs relative to the benefits of protecting the intellectual property;
- a human resources representative, who can coordinate personnel strategies (such as confidentiality agreements and exit interviews, discussed below) that are necessary to maintain trade secrecy; and
- a legal representative, who can speak to legal challenges that may arise in connection with the protection or use of the intellectual property.
So constituted, the IP committee can receive information from different departments across the company. This facilitates early decision-making as to whether an invention will be protected as a trade secret, through a patent application, or through some combination of the two, before any risk of disclosure. The IP committee also can advise as to why and how to achieve trade secret protection of certain information.

In addition to establishing IP committees, your business should **undertake a systematic approach to the documentation and categorization of trade secrets**. Once the company identifies information it would like to protect as a trade secret, you should proactively **gather evidence** regarding the cost of the information’s development and other indicia of its value, and ensure the company retains this evidence in a permanent database. You also should consider **preparing a workably specific definition of the trade secret**. Doing so will allow you to make a quick assessment as to whether a use or disclosure of your information may rise to the level of trade secret misappropriation.

At the same time, be careful how you identify the information, as the definition may be discoverable and could be used by a defendant to argue for a more limited scope of your trade secret rights. Consequently, to avoid creating a guidebook for an opposing party, **consider having an in-house attorney (or other party directed by counsel) prepare the definition** so that it can be protected under the work-product doctrine or attorney-client privilege. Further, you should **conduct regular audits** of trade secrets to ensure that your database is consistent with company practice. In any event, these and other organizational strategies will allow you to distinguish between ordinary confidential information (which must be protected through contract and tort doctrines) and trade secrets (which may be protected under the bodies of law discussed in this ACC Guide).

### B. Protecting Trade Secrets

Reasonable protective measures lay the groundwork for trade secret protection. Maintaining the secrecy of your company’s information can stop misappropriation before it happens—an ounce of security measures can be worth a pound of litigation. Moreover, legal classification as trade secret often begins and ends with the reasonable steps taken to protect that secret, so your protective scheme likely will play a central role in any litigation resulting from the misappropriation of your company’s trade secrets. Protective measures consist primarily of security policies aimed to prevent misappropriation, as well as confidentiality agreements and other contracts aimed to control and restrict the use or disclosure of information. This Subsection discusses each class of protective measures, how those measures have been treated in the case law, and how best to optimize your business’s efforts to protect its portfolio of trade secrets.

As discussed in Section II.C.3, above, trade secrets must be protected from every party that might handle the information and must receive some higher level of protection than other business information. In addition, your company’s employees with access to trade secrets should sign confidentiality agreements that survive the employees’ separation from your company, and your company should conduct exit interviews with any departing employee to secure the return of confidential materials, electronic devices, and other items.
These two practices form cornerstones of the protective measures analysis, as discussed in greater detail below.

A number of other baseline security measures can bear dividends for your company. Your business should limit access to information to a need-to-know basis and deploy common-sense security measures (locking your file cabinets, password-protecting your sensitive databases, etc.) to prevent unauthorized access to secret information. Your company also should prohibit employees from storing business information on their personal computers or cell phones, or at least require that employees secure any information stored on personal machines.

Similarly, your company should tailor its protective measures based on the company’s size and the value of the information. After all, the law only requires “reasonable” protective measures, and “reasonable steps for a two or three person shop may be different from reasonable steps for a larger company.”

Along those lines, as your company identifies workable protective measures, it should prepare an internal memorandum articulating its rationale for selecting (or not selecting) each measure considered. (Again, to prevent discovery of such internal documents, consider preparing them in a manner allowing them to be protected as privileged.) In addition to these standard rules, the case law marks a number of best practices to ensure that your business’s information has been sufficiently protected to qualify as trade secret.

Your company should systematically categorize its information based on its level of confidentiality. Although some businesses use complicated classification systems, a three-tier hierarchy usually will be sufficient:

- Tier one confidentiality might cover the bulk of your business’s information, and impose few, if any, restrictions on internal access and use.
- Tier two confidentiality covers information that your business aims to protect from its competitors, but may be willing to share with suppliers, vendors, potential customers, or other business partners under certain circumstances. Your business may decide to prohibit dissemination of tier two information unless the recipient has signed a confidentiality agreement.
- Tier three confidentiality covers any information that must stay completely internal to your business, such as source code, manufacturing processes, customer lists, business strategy information, and personnel information. Such information should be limited from disclosure to any outside party except under extraordinary circumstances.

Employees should be made aware of these categories and their significance, including through periodic internal training reminding them of the need for confidentiality.

Beyond categorizing its information, your company also should consider marking trade secret or other confidential information as such.
Marking policies make for powerful tools in the protection of your company’s trade secrets but can backfire if poorly implemented. By marking its documents as confidential, your company can ensure that anyone who views those documents understands that they contain protected information.242 Not only does this put employees on notice of the document’s secrecy, it also may help establish an implied duty of confidentiality, as sometimes required to show misappropriation.243

But marking cuts both ways, as courts take a failure to mark information as confidential as strong evidence that the information’s holder did not take reasonable measures to protect its secrecy.244 In short, although your company should consider marking policies as an additional safeguard for the secrecy of its information, it should only implement realistic policies likely to be followed by employees and other recipients of trade secret information on a systematic basis.

Your business also should limit departing employees’ access to confidential information. Employee departures constitute a recurring fact pattern in the trade secret case law, and these protective measures may prevent misappropriation in the first place.245 At a minimum, on the employee’s departure, your business should require that the employee return or delete any confidential information acquired during the employee’s tenure.246 Courts uniformly find that an employer destroys the trade secret protection of its information if it allows an employee to keep the company’s information when the employee leaves employment.247

Employees also should be informed of the confidential nature of your company’s information and, during onboarding, should be asked to sign a non-disclosure agreement (NDA) or other document in which they acknowledge the confidential nature of the information (as discussed in further detail below) and agree to maintain its confidentiality during employment and after separation.248

As an added layer of protection, your company’s Information Technology (IT) department should design protocols to automatically limit access to certain information by any employee who has submitted a notice of resignation, and the Human Resources (HR) department should take affirmative steps to ensure the return of proprietary company information after the employee departs. One such measure, the exit interview, is discussed in Section V.C., below.

Finally, your company should enter into NDAs or other agreements imposing a duty of confidentiality on any person or entity that receives access to your company’s trade secret information. Courts tend to treat such agreements as necessary, but not sufficient, for trade secret protection. Requiring execution of such an agreement, alone, does not establish that the business has taken reasonable protective measures,249 but courts take the failure to do so as strong evidence that the information at issue is not protected.250

Your company also may elect to require employees to execute non-competes or other restrictive covenants, such as customer non-solicitation agreements, as a method to restrict your competitors’ access to your trade secrets following an employee’s departure.
But because the enforceability of such agreements varies from jurisdiction to jurisdiction, restrictive covenants must be tailored to meet the requirements of local law. Moreover, because the law of restrictive covenants has evolved rapidly, a non-compete that worked five years ago, or even last year, may no longer be valid. This issue does not lend itself to a one-size-fits-all approach. Rather, as is the case with many other issues surrounding trade secrecy, you should work in concert with your company’s HR department to ensure that employment-related agreements comply with the rules in the applicable jurisdiction. In short, restrictive covenants should form only one aspect of your company’s protective measures.

Problems commonly arise where employees refuse to sign the confidentiality agreement. In *Yellowfin Yachts, Inc. v. Barker Boatworks, LLC*, for example, the US Court of Appeals for the Eleventh Circuit relied heavily on the defendant’s “refus[al] to sign an employment agreement which stated that he would, among other things, keep all Yellowfin trade secrets in confidence” in rejecting trade secret protection for the information. Consequently, your company should not allow employees to access confidential information if they refuse to sign confidentiality agreements. While inserting confidentiality provisions into an employee handbook is often helpful, there is no guarantee that an employee handbook can give rise to an enforceable confidentiality obligation on the part of an employee who refuses to sign a formal confidentiality agreement.

The expiration of your company’s NDAs or other confidentiality agreements also may present problems. In *Alta Devices, Inc. v. LG Electronics, Inc.*, discussed in Section II.G., above, the owner of the trade secrets narrowly avoided dismissal of its appropriation claim where the applicable NDA arguably had expired at the time of the misappropriation. As summed up by the Southern District of New York, “[o]nce a third party’s confidentiality obligation . . . expires, so does the trade secret protection.” To avoid this issue, any confidentiality agreement with an expiration date should provide for continued, post-expiration protection of any information your company contends constitutes a protectable trade secret that remains in effect as long as the trade secret information remains a trade secret. Incorporating such a survival provision into your company’s confidentiality agreements can help ensure that your trade secrets remain protected.

C. Enforcing Trade Secrets

At some point, your company likely will be called to enforce its rights in its trade secret information. No protective measure can ensure perfect security, and in the modern era of data breaches and employee mobility, opportunities for misappropriation inevitably will arise. By taking appropriate, swift action, you can limit your company’s exposure, reduce its legal spend, and, most importantly, help your company retain its rights in its trade secrets. This Subsection identifies strategies to minimize the need for litigation, as well as considerations to assess when deciding whether, when, and where to file suit.
I. Pre-Litigation Enforcement

You may be able to limit trade secret litigation by observing best practices as employees transition in and out of service with your company. Proper onboarding of employees can ensure that they leave behind any trade secrets they may have acquired from their previous work, helping limit your company’s misappropriation liability. Conversely, you should debrief and police the departure of any employee that leaves your firm to ensure that they do not bring your company’s trade secret information with them.

Similar but separate issues also may arise in dealings with vendors. If your company finds itself in a position where it must disclose its trade secrets to vendors, you should work with experienced trade secret practitioners to ensure that your company follows the best practices to preserve its trade secret rights. At a minimum, trade secrets should be disclosed to vendors only pursuant to the vendor’s contract confidentiality obligation that is without any durational limit.

When bringing in new hires, your company faces the risk that the new employee may use or disclose trade secret information acquired from a previous job. If the new hire does so, liability for misappropriation could extend to your company on a vicarious liability theory. Although the showing required to establish vicarious liability varies by jurisdiction, liability may attach if the new hire uses the trade secret information in furtherance of her job or discloses the information to her new coworkers.

To minimize the risk of vicarious liability, your company should establish an onboarding process for new hires. New hires should be warned against uploading any information from a former employer to your company’s computers, servers, or other electronic devices. This admonition also should be repeated in the employment agreement provided to any new employees hired by your company. Sample onboarding language for inclusion in your company’s employment agreement is included in the Appendix. In short, your company should make clear that any use of a prior employer’s trade secrets or confidential information is outside the scope of employment.

Your company also should develop departure procedures to help prevent misappropriation of your company’s trade secret information. In addition to the security measures discussed above to automatically protect against the misappropriation of trade secrets, your company should hold exit interviews with all departing employees. The interview serves to confirm that the employee knows he or she may not disclose any trade secret information acquired during their tenure and provides an opportunity for the return of any confidential information retained by the employee on their personal devices. After completion of the interview, you should have the departing employee sign an acknowledgement stating that you discussed these topics in the exit interview and that all confidential information, electronic devices, thumb drives, etc. have been returned. A sample exit interview form is attached in the Appendix.
2. Litigation

Despite the protective measures taken by your company, a sophisticated bad actor can frequently find a weakness to exploit. When misappropriation of your company’s trade secrets occurs, litigation can prevent further use or disclosure of the information. Litigation also opens the door to a variety of damages, offering your company a chance to be made whole. A solid understanding of the evidence needed and remedies available for a misappropriation action can allow your company to streamline its enforcement efforts and respond quickly to the misappropriation of its trade secret information.

Before filing suit, your company should gather the evidence necessary to enforce its trade secret rights. This requires the identification of specific evidence, not conclusory generalizations, establishing each element of trade secrecy. Be prepared to demonstrate (or at least allege facts that demonstrate) the independent value of the misappropriated information, the secrecy of and difficulty to ascertain that information, and the measures your company has taken to protect that information. Similarly, you should identify facts or reasonable inferences showing the bad actor’s acquisition, disclosure, or use of your company’s trade secret information, as well as the improper means or breached duty of confidentiality that allowed the bad actor to acquire your company’s information.

As a threshold matter, your company should prepare a litigation-ready definition of its trade secrets. Although the existence of a trade secret does not need to be pleaded with Rule 8 specificity, a plaintiff “must do more than simply list general categories of information” that allegedly qualify as trade secret. This endeavor requires trade secret plaintiffs to walk a tightrope in terms of the appropriate degree of specificity. If the definition “is too general, it will encompass material that the defendant will be able to show cannot be trade secret. If instead it is too specific, it may miss what the defendant is doing.” Moreover, the definition must avoid “general knowledge” possessed by a former employee, as well as “general secrets of the trade in which the [former] employee is engaged,” which do not qualify as trade secrets.

No approach to the specificity requirement has gained widespread acceptance. As a result, trade secret plaintiffs must familiarize themselves with the rules in the relevant jurisdiction and develop a strategy to meet the specificity requirement without painting themselves into a corner. If you cannot satisfy the specificity requirement without disclosing or otherwise jeopardizing your trade secrets, consider whether to seek leave to file a more fulsome description under seal.

Once the complaint is filed, you may need to continue refining the description of the subject information. “A number of states have enacted procedures requiring that trade secrets be identified before discovery commences.” One such procedure, which appears to be gaining in popularity, requires that trade secrets be identified with “reasonable particularity” before opening discovery. This entails “a description of the trade secrets at issue that is sufficient to (a) put a defendant on notice of the nature of the plaintiff’s claims and (b) enable the defendant to determine the relevancy of any requested discovery concerning its trade secrets.” Ideally, your company should be prepared to meet this standard before filing suit, although as a practical matter this goal may not be realistic.
Finally, while preparing to litigate, you should account for the need to seal some or all of your filings. Legal proceedings generally are public, so the failure to file information under seal will jeopardize its trade secret protection.270

As your company crafts its complaint, you should consider what relief may be available for the alleged misappropriation. Injunctive relief is particularly well-suited to trade secret litigation. After all, injunctive relief can maintain secrecy, and the loss of secrecy can mean the loss of trade secret protection.271 It does not follow, however, that misappropriation presumptively causes irreparable harm.272 As explained by the US Court of Appeals for the Second Circuit, a rebuttable presumption “might be warranted in cases where there is a danger that, unless enjoined, a misappropriator of trade secrets will disseminate those secrets to a wider audience or otherwise irreparably impair the value of those secrets.”273 But if a misappropriator “seeks only to use those secrets . . . in pursuit of profit, no such presumption is warranted because an award of damages will often provide a complete remedy for such an injury.”274 Similarly, although many NDAs specifically provide that disclosure of confidential information constitutes irreparable harm, many courts decline to give effect to such provisions.275 Thus, as with the other elements of your misappropriation claim, you should be prepared with hard facts or reasonable inferences showing the sort of irreparable harm required to obtain injunctive relief.

In addition to prohibiting further use or disclosure of the trade secret information, courts have read the UTSA to authorize injunctions preventing former employees from working for a competitor.276 As discussed above in Sections II.E. and III, under the inevitable disclosure doctrine courts may temporarily restrict or forbid employment with a competitor if the employment would result in the inevitable disclosure of trade secret information.277 Courts also have awarded similar remedies under the DTSA, even though that act expressly prohibits injunctions that “prevent a person from entering into an employment relationship.”278

In Waymo LLC v. Uber Technologies, Inc., a Waymo executive misappropriated some 14,000 confidential files regarding Waymo’s Light Detection and Ranging (LiDAR) system before accepting employment with Uber.279 Waymo sued, alleging misappropriation under both the California UTSA and the DTSA, and sought an injunction prohibiting the executive from working for Uber. The court granted an injunction, but declined to prohibit the executive from working for Uber altogether.280 Rather, the court ordered the executive to return all 14,000 confidential files, and prohibited him from performing any work pertaining to LiDAR.281 Thus, as shown by Waymo, your company may be able to obtain an order limiting the work performed by its ex-employee regardless of whether it sues under the UTSA or the DTSA.

In addition to injunctive relief, a variety of damages may be available as a remedy for misappropriation. The UTSA and DTSA authorize compensatory damages measured by the plaintiff’s actual loss in conjunction with the defendant’s unjust enrichment, or by a reasonable royalty for the misappropriated information. Attorneys’ fees and exemplary damages also may be awarded.
Courts in the United States frequently measure actual loss by the plaintiff’s lost profits—i.e., the profits that the plaintiff would have enjoyed had the defendant not misappropriated its trade secrets. Although decisions do not yield a one-size-fits-all approach, courts sometimes derive lost profits by multiplying the plaintiff’s profit margin by the defendant’s sales. Thus, if your profit margin is $60 per unit sold and the defendant sells 3,445 units of product built on your misappropriated trade secrets, you could establish lost profits in the amount of $207,000. Other metrics for actual loss include price erosion (the extent to which you reduced your prices in response to the misappropriated product), lost market share, and the plaintiff’s out-of-pocket expenses incurred as a result of the misappropriation.

A trade secret plaintiff also may be entitled to an award for the defendant’s unjust enrichment, provided that such an award does not result in a double recovery. Under the DTSA and UTSA, this measure of damages may include the defendant’s sales and avoided development costs. (New York courts, however, do not allow recovery of avoided development costs, on the theory that a plaintiff should not recover the defendant’s enrichment if the plaintiff has not suffered some loss due to that enrichment.) Once the plaintiff establishes its entitlement to unjust enrichment damages, the burden falls to the defendant to chip away at the amount of damages. The defendant, for example, may adduce evidence showing that some of its sales should not be attributed to the misappropriated trade secret, or that certain expenses should be deducted to determine the defendant’s net profits.

Regardless of the measure of actual loss, the trade secret plaintiff must establish a connection between the loss and the misappropriation. In one case, In re Jonatzke, the court rejected an expert witness’s estimate, based on the plaintiff’s price structure before and after the alleged misappropriation, that the plaintiff had suffered some $350,000 in price erosion damages. The expert did not account for “pricing trends in the [relevant] industry during this period of time” or any other “facts or data that might have influenced pricing during this time,” instead assuming the price erosion solely should be attributed to the defendant’s misappropriation. Consequently, the court rejected the testimony based on the expert’s failure to establish that the misappropriation caused the price erosion.

In addition, a trade secret plaintiff must tie its loss to the particular information misappropriated. In Texas Advanced Optoelectronic Solutions, Inc. v. Renesas Electronics America, Inc., the Federal Circuit vacated and remanded a jury verdict awarding more than $48 million in damages for misappropriation of three trade secrets. The Court of Appeals determined the defendant should only be held liable for misappropriating one of the three alleged trade secrets. In calculating the defendant’s unjust enrichment, the plaintiff’s expert “did not explain which of the trade secrets contributed to what amount of profit to be disgorged.” Rather, “he assigned all profits to the misappropriation of all trade secrets.” Because the record did not establish that the entire award could be attributed to the misappropriation of just one of the trade secrets, the Federal Circuit vacated and remanded for further proceedings.
If the plaintiff cannot establish the harm it suffered or profits the defendant enjoyed because of the misappropriation, the court may impose a reasonable royalty as an alternative measure of damages. Such a royalty, however, only may be awarded when the defendant actually used or disclosed the trade secret information; acquisition alone does not suffice. To determine the amount of a royalty, courts attempt to simulate a negotiation between the parties to license the trade secret at the time of its misappropriation. Most courts apply the “Georgia-Pacific factors,” drawn from the Southern District of New York’s patent infringement analysis in Georgia-Pacific Corp. v. U.S. Plywood Corp., to reach this amount. Notably, an empirical analysis of damages awards for misappropriation has shown that judges award reasonable royalties at a much higher dollar amount than do juries.

Finally, attorneys’ fees and exemplary damages also may be available under certain circumstances. Under the UTSA and DTSA, attorneys’ fees may be awarded to a defendant showing the frivolousness of a misappropriation claim, if the misappropriating party acted in bad faith to terminate or resist injunctive relief, or if the plaintiff shows willful or malicious misappropriation. In contrast, New York law only authorizes fees where the opposing party acted maliciously and was “entirely motivated by a disinterested malevolence.” Similarly, the UTSA and DTSA both authorize exemplary or punitive damages in cases of “willful and malicious misappropriation,” but limit such damages to twice the amount of compensatory damages. Although most states have adopted the UTSA standard for and cap on punitive damages, not all have done so. As a result, you should familiarize yourself with the statutes in effect in the relevant jurisdiction before seeking punitive damages.

VI. Conclusion

Trade secrecy offers a powerful tool to help your business protect its valuable intellectual property. Owing to its breadth and flexibility, trade secrets can play a number of roles in your company’s intellectual property portfolio. Customer lists, flowcharts, blueprints, negative know-how, manufacturing processes, and non-patented innovations all may be protected as trade secret. By identifying your valuable information before it has been misappropriated, gathering evidence establishing each element of its trade secret status, and taking reasonable measures to protect against your information’s disclosure, you can go a long way towards ensuring that your company maintains an edge over its competition.
VII. About the Authors

Joel Bush concentrates his practice in the area of complex commercial litigation, with particular emphasis on information technology and software disputes, misappropriation of trade secrets, commercial contracts, business torts, restrictive covenant, and technology license disputes. Mr. Bush has particular experience with trade secret issues involving software development, and he has litigated disputes arising out of computer hardware installations, software implementations, network design projects, and other technology implementations. More information about Mr. Bush may be found at https://www.kilpatricktownsend.com/en/People/B/BushJoelD.

Allen Garrett has significant experience in complex commercial litigation, arbitration, and appellate matters. Substantive areas of experience include antitrust and trade regulation, commercial contract disputes, consumer class actions (including "no injury" class actions), commercial insurance coverage disputes, enforcement of restrictive covenants, products liability, toxic torts, and trade secret litigation. His trial level experiences include state and federal court actions in numerous jurisdictions, as well as actions consolidated for pretrial proceedings by the Judicial Panel on Multidistrict Litigation. In recent years, Mr. Garrett has litigated a number of cutting-edge issues in connection with state consumer fraud statutes, federal jurisdictional disputes, and the protection of competitively valuable information. More information about Mr. Garrett may be found at https://www.kilpatricktownsend.com/en/People/G/GarrettCAllen.

Ben Richardson focuses his practice on complex commercial litigation, including class actions, commercial contracts, business torts, and trade secret litigation. Before joining Kilpatrick Townsend, Mr. Richardson was a judicial law clerk for Chief Judge W. Keith Watkins in the U.S. District Court for the Middle District of Alabama. More information about Mr. Richardson may be found at https://www.kilpatricktownsend.com/en/People/R/RichardsonBennettT.

The authors wish to thank David Chambers, Donald A. Gammon, Susanne Hollinger, and Casey Mangan, members of the Intellectual Property Network, for their outstanding editorial assistance and guidance.
VIII. Samples and Forms

A. Summary of Best Practices for Trade Secret Protection

1. Trade Secret Protection Plan: Identify Trade Secrets

The company should determine what information it possesses that gives the company an advantage over its competitors and, as such, might constitute the company’s trade secrets.

Examples of trade secrets include:

- Computer programs (including programmer’s notes)
- Business know-how (what works and what doesn’t)
- Specifications, bill of materials, recipes, and the like
- Processes (including flow charts)
- Formulas (including algorithms)
- Distribution sources
- Business methodologies
- Customer information (lists and preferences)
- Financial information
- Vendor/supplier lists (not readily available from public sources)
- Business and marketing plans
- Prototype products and test results
- Product/service pricing
- Personnel information
- Machinery (developed, utilized or unique to the company)

The following questions may help identify a company’s Trade Secrets:

- Is the information/process secret?
- Is the information/process valuable because it is secret?
- Is the information/process known in the industry?
- Is the information/process obvious to others or can they easily find it?

2. Conduct an Initial Trade Secret Audit

To ensure trade secret protection, routinely conduct an audit to determine (1) what measures are in place to secure trade secrets, (2) whether these measures are effective, and (3) what additional measures, if any, need to be put in place. The following questions can help organize an audit:
• Are there procedures in place to identify trade secrets as opposed to non-trade secret confidential information?
• Are there any measures currently in place to safeguard trade secrets that differ from those used to protect other confidential information?
• What are they?
• Where are the trade secrets located and is there a restriction on access to the location?
• Who has access to them?
• Are written policies concerning safeguarding trade secrets in place?
• Who signs nondisclosure agreements that would cover the trade secrets, when do they sign these, and what triggers the signature?
• What can be done further to safeguard trade secrets?

(3) **Develop a Trade Secret Protection Plan**

A trade secret protection plan should be in writing and reflect reasonable efforts under the circumstances to safeguard your organization’s trade secrets. Efforts to safeguard trade secret status are discussed in more detail in paragraphs 4-15 of this checklist.

4. **Segregate Trade Secrets**

Trade secrets should be segregated from non-trade secrets to differentiate between what the company regards as a trade secret and what it does not. By keeping the trade secret items/information separate from the non-trade secret items/information, the company’s claim of trade secret status has a much better chance of being preserved.

5. **Label Documents, Items and Software Containing Trade Secrets**

Label trade secret materials using the following or similar legends:

• “TRADE SECRET,” “SECRET,” “CONFIDENTIAL,” or “CONFIDENTIAL INFORMATION.”
• “TRADE SECRET. This document contains confidential and proprietary information of __[company name]__. Do not copy or circulate.”
• “CONFIDENTIAL INFORMATION. __[company name]__ (Unpublished) All rights reserved.”
• “PROPRIETARY INFORMATION. __[company name]__ (Unpublished) All rights reserved.”
• Create headers or footers on documents and software as follows: “This document contains confidential and proprietary information of __[company name]__ and is protected by copyright, trade secret and other State and Federal laws. Its receipt or possession does not convey any rights to reproduce, disclose its contents, or to manufacture, use or sell anything it may describe. Reproduction, disclosure, or use without specific written authorization of __[company name]__ is strictly forbidden.”
6. Nondisclosure Agreements

- All Employees, independent contractors, consultants, vendors, suppliers, licensees, and others that may, for any reason, access trade secrets should sign nondisclosure agreements.
- At a minimum, nondisclosure agreements should be signed by employees, consultants, contractors, vendors, and others who have access to (or will have access to) trade secret information and documents.
- Employees, consultants, contractors, vendors, etc., should sign nondisclosure agreements before the trade secret information/items are seen, discussed or revealed.
- Employees, consultants, etc. should read and sign the nondisclosure agreement on or before the first day of work

7. Employee Manual

If an Employee Manual exists, include:

- A section discussing the company’s Trade Secret Protection Plan and employees’ obligation under their Nondisclosure Agreements.
- Have employees sign a memorandum on the first day of employment that they have read the Employee Manual and understand the company’s Trade Secret Protection Plan.
- Place the memorandum in the employee’s personnel file.

8. Employee/Contractor Orientation and Education

Employees/Contractors should understand the elements and ramifications of the company’s Trade Secret Protection Plan from the first day of work.

- Mandate that new employees/contractors do not disclose the trade secrets of others (e.g., former employers).
- Explain that company trade secrets and confidential information cannot be disclosed outside the company.
- Make clear that disclosure of trade secrets and proprietary information are grounds for termination.
- Remind employees at their reviews of your Trade Secret Protection Plan and their duty under the Nondisclosure Agreement they signed.
- Discuss the company’s Trade Secret Protection Plan at employee meetings.
- Educate employees about industrial espionage/cybercrimes and help employees identify and report those who might attempt trade secret theft.
9. Notice Measures

Notice measures should be promulgated. Samples include:

- Routinely remind all persons of their obligations under the Nondisclosure Agreements.
- Routinely remind all employees of the company’s Trade Secret Protection Plan as discussed in the Employee Manual.
- Managers should confirm that key personnel can carry out the procedures set forth in the company’s Trade Secret Protection Plan.
- Distribute newsletter and/or memoranda that discuss the company’s Trade Secret Protection Plan.
- Place relevant posters in the workplace, such as in the employee lounge, kitchen or rest area.

10. Physical Security Barriers

All trade secrets should be kept from unauthorized persons as follows:

- Block access to persons who do not need to know.
- Keep trade secrets in a locked room with “Private,” “Authorized Personnel Only” or “No Admittance” posted on the door.
- Keep trade secrets under lock and key in appropriate file cabinets.
- Use a log to list who has access to the confidential information.
- Use access codes to enter buildings.
- Encode or encrypt trade secret information.
- Lock laptops and storage materials in safes or filing cabinets.
- Computers should have appropriate access codes, passwords and security software.
- Change access codes or passwords after an employee/contractor has left the company.
- Implement a clean desk policy.
- Where possible, maintain all confidential information out of sight.

11. Additional Steps to Keep Confidential Documents Secret

- Serialize and log trade secret documentation and materials.
- Safeguard all trade secret documentation and maintain careful chain-of-custody records when printing, delivering, or transmitting the documentation.
- Trade secret documentation should not be e-mailed. If a trade secret document must be e-mailed, use proper encryption technology and/or security keys. Additionally, mark the materials with the appropriate trade secret legends.
- If trade secret documents or software are duplicated by any means, a log should be kept showing who copied the document or software, and where the duplication is going.
- Shred all confidential documents that are duplications, are not needed or are no longer in use.
12. Prevent Dissemination of Trade Secrets or Confidential Information to Others

- Presentations, public speeches, web site information, press releases and all information that is to be disseminated to others should be scrutinized by the appropriate manager, so no trade secret is leaked or unwittingly disclosed.
- Employees, contractors, consultants, and others should be required to obtain permission if they desire to disclose or use information/items that may be confidential, proprietary or trade secrets.

13. Conduct Exit Interview with Departing Personnel

At employee/contractor exit interview:

- Review the terms of the nondisclosure agreement with departing personnel and ask him/her to contact the company if they have questions with respect to the nondisclosure agreement.
- Remind employee/contractor of duty not to use or divulge company’s trade secrets.
- Require that the employee sign a termination certificate, if possible, acknowledging employee’s/contractor’s understanding and duty not to disclose trade secrets or confidential information.
- Obtain trade secret materials and documents in the employee’s possession or control, including, without limitation, hard copies, diskettes (and other storage materials), home computer files, home office files, laptops, cell phones, etc.
- Require that keys and access cards be returned.

14. Visitors

Do not allow visitors (including repair or service persons) to wander freely. Incorporate the following procedures:

- Use a visitor’s logbook.
- Escort visitors.
- All trade secret/confidential information should be maintained out of sight at all times.
- Use nondisclosure agreements.
- Prohibit photography.
- Drape machinery that need not be seen.
- Maintain files out of sight.
- Restrict trade secret areas from access.

15. Conduct Routine Trade Secret Audits

- On a routine basis, establish a program to identify new trade secrets and modify existing trade secret descriptions as accurate and appropriate.
- Review the existing Trade Secret Protection Plan and update the plan as necessary.
B. Sample Trade Secret Policy

Scope

This policy sets forth procedures and measures to protect information identified as trade secrets owned by Company entities that shall affect all Company employees (herein, employee includes part and full time; temporary and permanent) and contractors.

Policy

1. Trade Secret Definition

A trade secret is information that is kept secret and provides economic value or a competitive advantage to Company because of its status as secret. Examples of information that could be considered a trade secret include information such as, but not limited to, formula, pattern, algorithm, compilation, program, method, technique, customer lists, data sets or compilations, product road maps, pricing schedules, failed experimentation, or manufacturing processes.

Information qualifying as a trade secret shall be identified as such by Company’s Intellectual Property (IP) committee and those employee(s) authorized to access the trade secret shall be responsible for maintaining its secrecy.

Factors that weigh into the consideration as to whether information should be considered a trade secret or Company confidential information or alternatively protected under other forms of IP are as follows:

- extent the information is known outside the business
- extent the information is known inside the business
- extent of measures that are used to guard the secrecy of the information
- ease or difficulty to reverse engineer
- value of the information to company and competitors
- effort/cost to develop information

In certain jurisdictions, the trade secret needs to be continuously used in the business.

2. On-Boarding Acknowledgement and Employment Agreements

a. At some point during the on-boarding process, an employee or contractor shall acknowledge that they will not use or disclose the trade secrets, inventions, and other proprietary and confidential information belonging to third parties. An acknowledgement form regarding third party trade secrets and proprietary information will be provided.
b. Before the employer/employee or employer/contractor relationship begins or meaningfully changes (e.g., by a promotion or assignment change) and before any trade secrets are disclosed, the employee or contractor shall sign an agreement that includes at least the following:

i. **IP Assignment**: Every employee or contractor shall sign an IP assignment. The agreement shall include a present assignment expressly transferring to the Company as the owner of IP, IP including trade secrets, developed by the employee during and in connection with his or her employment. A similar assignment also shall be signed by consultants, licensees, or other third parties where applicable.

ii. **Confidentiality Provision**: Every employee or contractor shall sign a Confidentiality Agreement acknowledging their duty of confidentiality with respect to Company’s information and trade secrets. A similar agreement also shall be signed by consultants, licensees, or other third parties.

iii. **Non-Compete/Non-solicitation**: To the extent permitted by law, the agreement shall contain provisions prohibiting an employee or contractor from accepting employment or performing services for a competitor or competing with Company or soliciting a former employer’s customers or employees.

For additional information, please consult the *Employee Handbook* and/or Human Resources (HR).

3. **Third Party Agreement**

Prior to entering a contractual relationship with a third party, a non-disclosure agreement (NDA) or agreement containing confidentiality provisions shall be executed before any Company confidential information - particularly trade secret information - is shared. If trade secrets are to be shared with third parties, kindly alert the Legal Department so additional contractual provisions may be included in the NDA or other agreement for added protection.

4. **Physical Security Measures**

a. **Facility Security Measures**: Access into and out of the facility shall be controlled and monitored with visitor sign-in logs with picture ID required, visitor non-disclosure agreements (NDA’s), pre-approval of all visitors, and surveillance cameras. All visitors shall be accompanied by an escort while on-site and are prohibited from on-site use of any device with recording capability (e.g., camera, video-camera, stop-watch or smart-phone with any of those functions).
b. **Restricted Access**: Access to the building shall be restricted through locked doors requiring badge entry issued to only authorized employees and contractors. All physical embodiments of a trade secret, whether a prototype, working model or actual embodiment in use, shall be maintained in a restricted area that is under lock and key and out of view. Employees or contractors shall put working materials or files containing trade secrets in a locked desk or filing cabinet when not in use (see *Clean Desk Policy*).

5. **Marking**

A trade secret shall be conspicuously marked as strictly confidential per our Global Marking Policy. This marking shall differentiate the trade secret information from other Company confidential information. Accordingly, for trade secret information all physical documents and digital files shall include “Company Strictly Confidential” either in the form of a header, footer or watermark. In any instance where trade secret information can be copied or downloaded, such copying of such document or digital files is tracked, monitored, and destroyed after use.

6. **Trade Secret Storage**

   a. **Identification and Description of Trade Secret**: Once information has been identified as trade secret, the Company IP attorney will prepare a brief description of the trade secret. This ensures the description of the trade secret is protected under attorney-client privilege.

   b. **Protective Measures**: Trade secrets will be maintained and protected in a manner that is greater than that of Company confidential information. All trade secrets shall be stored in a trade secret database on a Company controlled network that is password protected where the password is known only to Authorized Persons (defined in Section 7 herein). Additional encryption measures may be used where appropriate. The database shall be maintained by a Company IP attorney and/or Information Technology (IT) where access is granted. Trade secrets shall be segregated from other Company confidential information and only accessible through a Company-controlled network and not through any other network, cloud storage, or the internet except via the Company Internal Private Network (VPN). Old hardware, such as laptops or hard drives containing trade secret information, should be physically destroyed rather than being thrown away or recycled.

7. **Limited, Need-to-Know Access**

   a. **Responsible Employee**: Employee(s), as designated by a Company US IP attorney or the Company IP committee, shall be responsible for maintaining the secrecy of each trade secret by ensuring that the requirements of this policy are met for that trade secret.
b. **Authorized Persons Only**: Access or use of a trade secret by an authorized person is authorized only if, and only to the extent, he or she needs to access or use the trade secret to perform his or her job responsibilities. An authorized person may copy a trade secret, or a portion of a trade secret, only if necessary, to perform his or her job responsibilities. All such copies shall be promptly destroyed, i.e. rendered indecipherable and unable to be reconstructed once they are no longer needed.

c. Visitors must sign acknowledgments prohibiting disclosure of information viewed or accessed during a visit, preventing them from bringing recording devices (e.g., cameras, cell phones, USB drives) into restricted areas, and requiring that they be accompanied by employees while in locations where they may access sensitive information.

d. **Electronic Information Management**:  
   i. Access to trade secrets shall be limited to only authorized persons and through only authorized means.
   
   ii. If information relating to a trade secret must be shared between authorized persons, it shall be done through secure transfer means, i.e. via encrypted email or a secure file transfer.
   
   iii. A list of the persons authorized to access a trade secret shall be maintained by the Responsible Employee for each trade secret and/or the Company IP Attorney.

8. **Protected Networks and Mobile Devices**

   a. **Network and Device Security**: Network and device security solutions shall be maintained by Company’s IT department as in the normal course of business.

   b. **Personal Devices**: Employees and contractors shall follow Company’s policies regarding use of company devices that precludes employers and contractors from using personal devices for work related matters unless he or she has complied with Company’s *Bring Your Own Device (BYOD) Policy*. **Downloading or use of trade secret information on personal devices is prohibited.**

   c. **Portable Device or Drives**: Portable devices or drives are not allowed for use on Company computers.

9. **Proprietary Data Control**

All presentations, articles, and research papers that are to be publicly disclosed, or otherwise disclosed to non-employees, shall be reviewed by a Company IP attorney prior to the disclosure, so that trade secrets and any other Company confidential information are not disclosed.
10. Employee Training

Employees and contractors shall receive IP training as a part of Company’s New Hire Orientation, as applicable. The IP training portion shall include the topics of trade secrets and Company’s trade secret policy. Thereafter, employees and contractors shall have periodic certifications and policy acknowledgements of IP and Trade Secret Policy training.

11. Off-Boarding Process

Exit interviews shall be conducted for all employees and contractors who have been terminated or are otherwise departing Company. During the exit interview, at least the following steps will be performed:

a. Upon resignation or termination, Company IT shall be alerted, and the departing employee or contractor shall have their e-mail access and network access disabled. All employee or contractor passwords shall be terminated. Any laptops, phones, or other company provided devices will be retrieved by IT, and employee or contractor shall sign an acknowledgment that all company-provided laptops, documents, etc. have been returned.

b. The employee or contractor shall be provided with a copy of the agreements from Section 2 herein, including the Confidentiality Agreement which references the employee’s or contractor’s continuing duty to keep trade secrets (and other Company confidential information) confidential. The employee or contractor will be reminded of their continuing duty with respect to Company confidential information and trade secrets and shall sign an acknowledgement of such reminder.

c. Access keys, keys to desks or cabinets, company credit card, and/or key cards shall be returned to Building Security and/or Human Resources (HR).

d. Any laboratory or engineering notebooks shall be retrieved and inventoried by the Company IP department. The Company IP attorney shall remove the employee from any authorization lists.

e. If a personal device was used for work related duties, it shall be cleansed of any sensitive company information.

f. Request IT to monitor any downloads of Company information via portable devices by departing employee and/or e-mails to employee personal e-mail or out of Company network account.

An Exit Interview Form (to be completed prior to employee or contractor departure) should be used as part of the off-boarding process. For additional information, please consult the Employee Handbook and/or Human Resources (HR).
12. Remedies for Trade Secret Misappropriation

Trade secret misappropriation is governed by State (or in Canada Provincial) and Federal laws. Remedies for trade secret misappropriation may include injunctive relief, monetary damages, attorneys’ fees, litigation costs, and in some cases, criminal sanctions including fines and imprisonment.


An employee or contractor will be immune from an action that would otherwise count as trade secret misappropriation if the disclosure is made (i) in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney; and (ii) solely for the purpose of reporting or investigating a suspected violation of law; or is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal. (18 U.S.C. 1833(b)).

This notice shall be included in Confidentiality or Non-Disclosure Agreements and NDAs entered by Company described in Section 2 herein.

Related Policies:

Employee Handbook

Clean Desk Policy

Bring Your Own Device (BYOD)

Global Marking Policy – Confidential Information
C. Possible “Notice” Language About Whistleblower Immunity

- You are hereby notified in accordance with the Defend Trade Secrets Act of 2016 that you will not be held criminally or civilly liable under any federal or state trade secret law for the disclosure of a trade secret that (a) is made (i) in confidence to a federal, state, or local government official, either directly or indirectly, or to an attorney; and (ii) solely for the purpose of reporting or investigating a suspected violation of the law; or (b) is made in a complaint or other document that is filed under seal in a lawsuit or other proceeding.

- You are further notified that if you file a lawsuit for retaliation by an employer for reporting a suspected violation of law, you may disclose the employer’s trade secrets to your attorney and use the trade secret information in the court proceeding if you (a) file any document containing the trade secret under seal; and (b) do not disclose the trade secret, except pursuant to court order.
D. Sample Acknowledgement Regarding Trade Secrets and Proprietary Information for Incoming Employees

I understand and acknowledge that it is the policy of X Company and its affiliates (the “Company”) to respect the trade secrets, inventions, and other proprietary and confidential information (“Confidential Information”) belonging to third parties. Therefore, in addition to agreeing not to disclose or use Confidential Information belonging to the Company in violation of any applicable confidentiality agreement or Company policies as may be in effect or amended from time to time, as a condition of employment with the Company, I hereby represent and agree as follows:

1. I am not subject to any agreement of any kind with any prior employer or other person or entity relating in any way to my right or my ability to be employed by and/or to perform services for the Company.

2. The Company has instructed me not to bring to, disclose to or use in connection with my employment or potential employment with the Company any Confidential Information from any prior employer or other person or entity.

3. I have not brought to, disclosed to or used in connection with my employment or potential employment with the Company any Confidential Information from any prior employer or other person or entity.

4. I will not bring to, disclose to or use in connection with my employment with the Company any Confidential Information from any prior employer or other person or entity.

5. During my employment with the Company and thereafter, I will not take, disclose or use any Confidential Information acquired as a result of my employment with the Company, except as authorized by the Company.

________________________________________
Employee’s Printed Name

________________________________________
Employee’s Signature

________________________________________
Date
E. Sample Exit Interview Form

(TO BE COMPLETED PRIOR TO DEPARTURE)

INTRODUCTION

We understand that you will be ending your employment with the Company on _____________ [date]. You remain a Company employee until that date and should not begin performing any work for your new employer until after that date, whether during or after business hours. As you prepare to leave, we ask that you complete this Exit Interview/Checkout Form. It will assist us in processing your exit and accounting for various types of Company property you may have received prior to your departure.

EQUIPMENT AND ACCESS TOOLS

We need to ensure that all of our equipment has been returned to the Company, please respond to the following:

<table>
<thead>
<tr>
<th></th>
<th>Returned?</th>
<th>Never Issued</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Identification Card</td>
<td>Yes ☐</td>
<td>No ☐</td>
</tr>
<tr>
<td>2. Corporate Credit Card</td>
<td>Yes ☐</td>
<td>No ☐</td>
</tr>
<tr>
<td>3. Facility Access Card/Keys</td>
<td>Yes ☐</td>
<td>No ☐</td>
</tr>
<tr>
<td>4. Corporate Calling Card</td>
<td>Yes ☐</td>
<td>No ☐</td>
</tr>
<tr>
<td>5. Company Cell Phone</td>
<td>Yes ☐</td>
<td>No ☐</td>
</tr>
<tr>
<td>6. Company Laptop or Other Computer Equipment</td>
<td>Yes ☐</td>
<td>No ☐</td>
</tr>
<tr>
<td>7. Company Thumb Drive/Zip Drive/External Hard Drive</td>
<td>Yes ☐</td>
<td>No ☐</td>
</tr>
<tr>
<td>8. Company iPad/Tablet</td>
<td>Yes ☐</td>
<td>No ☐</td>
</tr>
<tr>
<td>9. Other</td>
<td>Yes ☐</td>
<td>No ☐</td>
</tr>
</tbody>
</table>

Initials _______

Wiped?

Personal mobile device(s) | Yes ☐ | No ☐ |

Initials _______
DOCUMENTS/FILES/RECORDS

As an employee of X Company, you had access to various documents, reports, and information that the Company considers proprietary and confidential – in both electronic and paper form. The Company needs to confirm that all of its property has been returned or deleted from non-Company storage media (CDs/DVDs, portable hard drives, thumb drives, personal handheld devices, cell phones, smart phones, personal e-mail accounts, personal desktop computers, personal laptop computers, and the like) and that none of these items have been disclosed to persons outside of the Company. We have listed below some of the most confidential documents of the Company; by listing some documents here but not others we do not mean to suggest that other Company documents are not confidential. Please respond to the following:

Examples of Documents – Have You Received or Been Given Access to the Following Materials?

1. [Annual Strategic or Sales Plan] Yes ☐ No ☐
2. [Customer List] Yes ☐ No ☐
3. [Customer Profiles] Yes ☐ No ☐
4. [Research Notebooks or Plans] Yes ☐ No ☐
5. [Other relevant core Company documents] Yes ☐ No ☐

*Did you copy or e-mail any of these documents? Yes ☐ No ☐

*Did you disclose or transfer any of this information to anyone outside of the Company? Yes ☐ No ☐

*Are you currently in possession of any of these documents? Yes ☐ No ☐

*If the answer to any of these questions is yes, please explain:

________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
If during the course of your employment, you transferred any Company documents (not limited to the documents listed above) to non-Company storage media (such as CDs/DVDs, portable hard drives, thumb drives, and the like), personal handheld devices, cell phones, smart phones, personal e-mail accounts, or personal desktop or laptop computers, please identify all such media, devices, e-mail accounts, or computers and their location. We will discuss with you how to ensure that all such materials are returned or properly deleted from non-Company media.

________________________________________________________________________

Have you returned all X Company confidential and proprietary documents? Yes ☐

If so, to whom, when, and how? ________________________________ No ☐

________________________________________________________________________

Initials _____

CODE OF CONDUCT

As you know, the Company takes its Code of Conduct very seriously. The Code of Conduct provides, among other things, that employees shall not use corporate property or information for personal gain. You have acknowledged your compliance with this Code. A copy is attached.

Initials _____

EMPLOYEE INVENTION AND TRADE SECRET AGREEMENT

As you know, your relationship with the Company is governed by an Employee Invention and Trade Secret Agreement you entered into with the Company (copy attached). This Agreement provides that, in your employment after leaving, you will not disclose, without the Company’s written consent, any secret or confidential information obtained during your employment with the Company.

Based on your commitments to the Company, there may be situations in the course of your new employment in which you simply cannot participate in a project without necessarily using the confidential information you have learned about the Company. In those situations, your agreement with the Company requires that you excuse yourself from those specific projects.
In other circumstances, it may be most effective for you to simply assign responsibility for particular projects to other individuals, acting without your guidance. There may be situations in which you are not certain whether information you know and would like to use in your work with your new employer is in fact confidential information of the Company. In those circumstances, we ask that you contact the Company to discuss the issue and arrive at an appropriate resolution that will respect your continuing obligations to the Company.

Your obligation not to disclose, without the Company’s prior written consent, any secret information obtained during the course of your employment with the Company, remains in effect for as long as such information remains a trade secret under applicable law.

Your obligation not to disclose, without the Company’s prior written consent, any confidential or proprietary information obtained during the course of your employment with the Company, remains in effect for [INSERT SET TERM FROM AGREEMENT] years.

Initials ______

OTHER AGREEMENTS

Your post-employment obligations are also governed by the [INSERT NAME OF AGREEMENT]. A copy of this Agreement is attached. If you have any questions about this Agreement, please contact ___________________________.

Initials ______

NEW EMPLOYMENT

Have you accepted other employment?

If so, with what company? ______________________________

What will be your new title? ______________________________

When is your anticipated start date? __________________________

What is your contact information? (phone, email and physical address)?

Phone: ___________________________________________

Email: ___________________________________________

Address: __________________________________________

Initials ______
Please take a moment to ensure that your answers above are accurate. Again, we thank you for completing this form and assisting with our on-going efforts to protect our confidential and proprietary information. We thank you for your services.

Dated: ______________________

[Executive Signature]

[Print Name]
IX. Endnotes

1 See, e.g., Unif. Trade Secrets Act § 1(4).
3 Id.
5 Veronica Foods Co. v. Ecklin, No. 16-CV-07223-JCS, 2017 WL 2806706, at *12-13 (N.D. Cal. June 29, 2017) (“Due to the overlap between the statutes, several courts have addressed DTSA claims in conjunction with claims under the [California Uniform Trade Secrets Act] and other states’ versions of the Uniform Trade Secrets Act.”).
10 Almeling, supra note 8, at 1104.
13 See id.
14 Almeling, supra note 8, at 1106.
15 See, e.g., Ashland Mgmt, 82 N.Y.2d at 407, 624 N.E.2d at 1012-13, 604 N.Y.S.2d at 917-18.
16 An Act to Amend the General Business Law and the Civil Practice Law and Rules, in Relation to the Uniform Trade Secrets Act, S.B. 2468 (2020).
17 18 U.S.C. § 1836; see also Elizabeth A. Rowe, Snapshot of Trade Secret Developments, 60 Wm. & Mary L. Rev. 45, 48 (2019).
18 Rowe, supra note 17, at 49.
20 Rowe, supra note 17, at 49.
23 See generally Sandeen, supra note 6.
24 See id. at 454-59.
25 See generally id. (discussing international efforts to harmonize trade secret law across
jurisdictions).


28 See id.

29 Id. art. 39(2).

30 Id. art. 39(2) n.10.

31 Id. art. 39(3).

32 Id.

33 Id.

34 Scott J. Shackelford, et al., Using Bits to Protect Bytes: Promoting Cyber Peace by Safeguarding Trade Secrets Through Bilateral Investment Treaties, 52 Am. Bus. L.J. 1, 33 (2015) (discussing a bilateral investment treaty between the United States and Poland requiring that Poland “provide adequate and effective protection for propriety information . . . [that] has actual or potential economic value from not being generally known”).


37 E.g., Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174 (7th Cir. 1991).


39 Id. at 996.

40 Id. (emphasis in original).

41 Id.


43 Id. at 295, 106 N.E.3d at 8.

44 Id. at 297, 106 N.E.3d at 9.

45 Id.

46 Id. at 298, 106 N.E.3d at 10.

47 Penalty Kick Mgmt. Ltd. v. Coca Cola Co., 318 F.3d 1284, 1291-92 (11th Cir. 2003) (holding that combination of public domain elements with proprietary information in “an effective, successful and valuable” manner constituted a trade secret).

48 Unif. Trade Secrets Act § 1(4)(i); see also 18 U.S.C. § 1839(3) (excluding information readily ascertainable by “another person who can obtain economic value from its disclosure or use” from the definition of trade secrets).


50 Id. at 252, 252 n.2.

51 Id. at 253 (alterations and internal quotation marks omitted).

52 Id. at 253, 254 n.4.

53 Id. at 253.

54 Id. at 254 (emphasis in original).

55 Id. at 254 (emphasis in original).


57 Id. at *4-5.

58 Id. at *5.

59 Id.

60 Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 180 (7th Cir. 1991) (Posner, J.).


Id. at 517.


Id.

Id. at *5.


Id.

Id.

Id.

Xerox Corp., 2006 WL 3053408, at *9 (holding Xerox established a likelihood of success on the merits of its unfair competition claim where it showed that it “spent millions of dollars developing and maintaining its [customer] database,” which was comprised of information “not generally known outside of Xerox,” which was “not shared with Xerox dealers” and was “divulged to Xerox employees and agents [only] under strict conditions”).

La Calhene, Inc. v. Spolyar, 938 F. Supp. 523, 530 (W.D. Wis. 1996) (finding “strategic and marketing plans” were protectable trade secrets where the plans were kept confidential and reflected information “highly valuable to competitors . . . [and was] the product of time and effort on the part of plaintiff”).


Id. at *7.

Id. at *6-7.

Id.


Id. at 493.

Id. at 492.

Cf. Data Gen. Corp. v. Digital Computer Controls, Inc., 297 A.2d 433, 436 (Del. Ch. 1971) (holding that widespread disclosure of computer design drawings did not preclude trade secrecy of those drawings because the disclosures were made subject to agreements requiring confidentiality), aff’d, 297 A.2d 437 (Del. 1972).

See id.


E.g., AirFacts, Inc. v. de Amezaga, 909 F.3d 84, 96-97 (4th Cir. 2018).

Id. at 88.

Id. at 96.

92 See, e.g., Brand Servs., LLC v. Irex Corp., 909 F.3d 151, 157 (5th Cir. 2018) (holding that, although the UTSA preempts certain tort claims that are based on the same facts as misappropriation of trade secrets, such tort remedies remain available for theft of confidential information that does not otherwise qualify as trade secret).

93 Unif. Trade Secrets Act § 1(2).

94 Id. § 1(1).

95 431 F.2d 1012, 1015-16 (5th Cir. 1970).

96 Id. at 1016 (explaining that the policy in favor of “freewheeling industrial competition must not force us into accepting the law of the jungle as the standard of morality expected in our commercial relations”).


98 See, e.g., Centrifugal Acquisition Corp. v. Moon, 849 F. Supp. 2d 814, 833 (E.D. Wis. 2012) (implying a duty of confidentiality where employee gained “‘intimate’ working knowledge of [employer’s] ‘unique’ process” over years of work).

99 Id.

100 E.g., Smith v. Dravo Corp., 203 F.2d 369, 376 (7th Cir. 1953).

101 See generally Godfrey, supra note 67, at 165.


103 Id.

104 Unif. Trade Secrets Act § 3(a).

105 Unif. Trade Secrets Act § 3(b).

106 Unif. Trade Secrets Act § 2(a).


110 Epstein v. C.R. Bard, Inc., 460 F.3d 183, 188 (1st Cir. 2006).


112 Id. at 511-12, 644 S.E.2d at 351.

113 Id. at 514, 644 S.E.2d at 352.

114 Id. at 517-18, 644 S.E.2d at 354-55.

115 Id. at 517, 644 S.E.2d at 354.

116 Id.

117 Id. at 519, 644 S.E.2d at 356.

118 Id. at 519, 644 S.E.2d at 356.


120 Id. at 307.

121 Id. at 309.

122 Id. at 315

123 Id. at 312.

124 Id. at 316.
Id. at 315; see also id. at 315-16 (“It was not the world’s burden to unearth facts relating to [the competing inhibitor manufacturer’s] identity, its relationship with [Miller’s former employee], and its role in profiting from the allegedly stolen formula. That burden was Miller’s.”).


O.C.G.A. § 10-1-766. Note that Georgia applies the statute differently depending on whether the claim is asserted against one person for continuing misappropriation or against others who “receive[d] [the] trade secret from another person who misappropriated that trade secret.” Id.


See Ashland, 82 N.Y.2d at 407, 624 N.E.2d at 1013, 604 N.Y.S.2d at 918. Specifically, courts consider “(1) the extent to which the information is known outside of [the] business; (2) the extent to which it is known by employees and others involved in [the] business; (3) the extent of measures taken by [the business] to guard the secrecy of the information; (4) the value of the information to [the business] and [its] competitors; (5) the amount of effort or money expended by [the business] in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.” Id. (alterations in original) (citing Restatement (First) of Torts § 757 cmt. b (1939)).

Id.


See Ashland, 82 N.Y.2d at 407, 624 N.E.2d at 1013, 604 N.Y.S.2d at 918.

Id.


Id. at 737 (alteration omitted).


Almeling, supra note 8, at 1101-04. See also Magdalena Kolassa, Trade Secrets and Employee Mobility: In Search of An Equilibrium, Cambridge International Property and Information
When a trade secret is disclosed under a time-limited obligation, rather than a perpetual obligation to keep it confidential, court have found that the trade secret was not subject to reasonable efforts to maintain its secrecy and therefore is no longer entitled to trade secret protection. DB Riley, Inc. v. AB Engineering Corp., 977 F. Supp. 84 (D. Mass. 1997) (finding no trade secret protection when disclosure was made under a time-limited confidentiality agreement, which confirmed plaintiff’s “own expectations of maintaining its trade secrets were time limited.”); see also Silicon Image, Inc. v. Analogix Semiconductor, Inc., No. C-07-00635 JCS, 2008 WL 166950, at *17 (N.D. Cal. Jan. 17, 2008) (internal citation omitted) (“courts have denied trade secret protection whe[n] allegedly confidential information has been revealed to third parties without protections that are considered adequate, for example, where the information was disclosed under a non-disclosure agreement with only a limited duration.”). Relying on these cases, Judge Rakoff (S.D.N.Y.) found that trade secret protection cannot extend to information disclosed under a time-limited confidentiality agreement. Structured Capital Solutions, LLC v. Commerzbank AG, 177 F. Supp. 3d 816, 835 (S.D.N.Y. 2016), citing DB Riley and Silicon Image. “[A] temporary pledge to secrecy is exactly that: temporary. Once a … confidentiality obligation … expires, so does the trade secret protection.” Id. at 836.

See Almeling, supra note 8, at 1098-1100.

See id. at 1110-12.

Rowe, supra note 17, at 49.

Rowe, supra note 17, at 48.


Elizabeth A. Rowe, Unpacking Trade Secret Damages, 55 Hous. L. Rev. 155, 183 (2017)

Id. § 1836(d).

Rowe, supra note 17, at 49; see also, e.g., Yeiser Research & Dev., LLC v. Teknor Apex Co., No. 17-cv-1290, 2019 WL 2177658, at *4 (S.D. Cal. May 20, 2019); but see Earthbound Corp. v. MiTek USA, Inc., No. 16-cv-1150, 2016 WL 4418013, at *10 (W.D. Wash. Aug. 19, 2016) (explaining that the DTSA “defines trade secrets similarly to but even more broadly than the UTSA”).

Alta Devices, 343 F. Supp. 3d at 877.

Camick v. Holladay, 758 F. App’x 640, 644-45 (10th Cir. 2018).


See id. § 1836(c).


See Motorola Sols., Inc. v. Hytera Comms’ns Corp., 436 F. Supp. 3d 1150, 1159-63 (N.D. Ill. 2020) (holding the DTSA applies extraterritorially; analyzing the issue at length after declining to “join the chorus of district courts that have held [as much] without discussion”).


Id. at 1165.

Id. at 1166.

54 F.3d 1262, 1268 (7th Cir. 1995).

Id. at 1270 (comparing PepsiCo to a “a coach, one of whose players has left, playbook in hand, to join the opposing team before the big game”).

Id. at 1272 (relying in part on “the district court’s reluctance to believe that [the executive] would refrain from disclosing these secrets in his new position (or that Quaker would ensure [the executive] did not disclose them”)’).


690 F. App’x 72, 76 (3d Cir. 2017).

Id.


Id. (citing Whyte v. Schlage Lock Co., 101 Cal. App. 4th 1443, 1463 (2002)).


Id.


Id. at *1 (discussing the entry of “an ex parte temporary restraining order authorizing the seizure of a laptop computer” alleged to contain the movant’s trade secrets).


Id. § 1836(b)(3)(B).

Id. § 1836(b)(3)(C).

Almeling, supra note 8, at 1112.

See Penalty Kick, 318 F.3d at 1292 (explaining that information included in a patent application was not protectable as trade secret).


Id. § 102(a).

Id. § 103.

See, e.g., Experian Info. Sols., 893 F.3d at 1189.


See id.

Flexible Techs., 2019 WL 1417465, at *3.

See Almeling, supra note 8, at 1115-16.


Id. (discussing an award by a Tokyo court of 330 million yen to a Japanese inventor who patented a click wheel similar to the iPod’s several years before it was developed by Apple).

E.g., MEI-GSR Holdings, 416 P.3d at 252-54.

See Almeling, supra note 8, at 1112-14.

That said, your company should beware of claiming trade secret protection for information implicating the “best mode” to carry out its patented invention. Because patent law requires applicants to disclose the best mode to use their patentable inventions, withholding information concerning the best mode in an attempt to maintain trade secrecy may lead to rejection of your application or invalidation of your patent. See, e.g., Chemcast Corp. v. Arco Indus. Corp., 913 F.2d 923, 930 (Fed. Cir. 1990) (affirming invalidation of patent where manufacturer failed to disclose the best mode to carry out its invention).

See Flexible Techs., 2019 WL 1417465, at *3.

See, e.g., Liqwd Inc., No. 1:17-cv-14-JFB-SRF (D. Del.), ECF No. 1060 (reflecting awards of approximately $47 million for patent infringement, $22 million for trade secret misappropriation, and $22 million for breach of confidentiality agreement).

See Almeling, supra note 8, at 1104-06.

Cf. Cy Wakeman, 284 F. Supp. 3d at 996 (denying preliminary injunction where movant could not establish independent economic value of allegedly trade secret information).
For instance, your company could develop a trade secret manufacturing process for one chemical that, years later, it discovers can be modified to produce a second chemical. If your company initially defined the trade secret as encompassing only the production of the first chemical and neglected to update the definition to include production of the second chemical, a defendant could use the outdated definition to argue that the manufacturing process for the second chemical does not qualify as a trade secret because the second chemical was not included in the company’s internal identification of trade secrets.


Opus Fund, 2018 WL 1156246, at *3.


Id. (alteration omitted).


See Wrap-N-Pack, Inc. v. Eisenberg, No. 04-cv-4887 (DRH) (JO), 2007 WL 952069, at *9 (E.D.N.Y. Mar. 29, 2007) (remarking favorably on company’s “significant safeguards to protect its customer information” where, among other things, “the Company reminded salesmen of their duty and obligation to maintain customer confidentiality via office memoranda”).

See Orthofix, Inc. v. Hunter, 55 F. Supp. 3d 1005, 1012-14 (N.D. Ohio 2014) (finding company failed to take sufficient steps to protect its allegedly trade secret information where, among other things, employee never was informed as to “what information was deemed ‘confidential’ under [his] employment agreement”), rev’d on other grounds and remanded, 630 F. App’x 566 (6th Cir. 2015).

Cf. Centrifugal Acquisition Corp., 849 F. Supp. 2d at 833 (explaining that a duty of confidentiality may be implied where the recipient of information “knew or had reason to know that the disclosure was intended to be in confidence,” and finding that such a duty arose where employee understood information to be “the confidential and proprietary property of [his employer]”).

E.g., Convolve Inc. v. Compaq Computer Corp., 527 F. App’x 910, 921-22 (Fed. Cir. 2013) (holding allegedly trade secret information “lost any trade secret status it might have had” after it was disclosed but not marked as confidential as required by the NDA governing the information’s disclosure); Call One, Inc. v. Anzine, No. 18-cv-124, 2018 WL 2735089, at *8-*9 (N.D. Ill. June 7, 2018) (granting summary judgment in favor of former employee on misappropriation claim, reasoning that no duty of confidentiality was owed as to a document “not actually identified as being confidential, given [the employer’s] own requirement that all confidential information and trade secrets be marked as such”).

See, e.g., Cerro Fabricated Prods., 300 F. Supp. 3d 632.

Yellowfin Yachts, Inc. v. Barker Boatworks, LLC, 898 F.3d 1279, 1300 (11th Cir. 2018) (affirming summary judgment in favor of employee where employer “did not request that [the employee] return or delete any of the [confidential] information” he had acquired from
his employer prior to his departure).

247 E.g., Capitol Comm’n, Inc. v. Capitol Ministries, No. 5:11-cv-214-BO, 2013 WL 5493013, at *4 (E.D.N.C. Oct. 2, 2013) (finding employer could not establish reasonable measures to maintain information’s secrecy where it “granted permission for each state minister that left its employ to take [the allegedly trade secret information] with him”).

248 See Yellowfin Yachts, 898 F.3d at 1300-01.

249 Opus Fund, 2018 WL 1156246, at *3 (“While an agreement restricting the use of information may be considered a reasonable step to maintain secrecy of a trade secret, such an agreement, without more, is not enough.”) (quoting Fire ‘Em Up, Inc. v. Technocarb Equip. (2004) Ltd., 799 F. Supp. 2d 846, 851 (N.D. Ill. 2011)).


251 See, e.g., Mass. Gen. Laws c. 149, § 24L(b) (imposing requirements for enforceability of non-compete); id. § 24L(e) (requiring that Massachusetts law be applied to determine the enforceability of a non-compete purportedly applicable to a person residing or working in Massachusetts).

252 898 F.3d at 1300.

253 See Art & Cook, Inc. v. Haber, 416 F. Supp. 3d 191, 197 (E.D.N.Y. 2017) (finding reasonable measures were not taken where employer “did not ask Defendant to sign the employee handbook and non-disclosure agreement until three years into his employment,” and gave the defendant access to allegedly confidential information even though “Defendant refused to sign either document”).

254 E.g., Wrap-N-Pack, 2007 WL 952069, at *9 (citing with approval the trade secret claimant’s use of an “employee policy-and-procedure manual . . . that contained a code of conduct defining unacceptable behavior to include disclosing confidential information”).

255 343 F. Supp. 3d at 879-80.

256 Structured Capital Sols., LLC v. Commerzbank AG, 177 F. Supp. 3d 816, 836 (S.D.N.Y. 2016) (holding information did not qualify as trade secret where it was disclosed under a confidentiality agreement that had since expired).


DeRubeis, 244 F.R.D. at 681 (bemoaning the lack of a “talismanic procedure the Court may apply in order to obtain the best result in any given case”).

Elsevier, 2018 WL 557906, at *6 (referencing such a procedure with approval).


Id.


E.g., FMC Corp. v. Taiwan Tainan Giant Indus. Co., 730 F.2d 61, 63 (2d Cir. 1984) (“A trade secret, once lost is, of course, lost forever”); see also Nat’l Fish & Seafood, 2018 WL 4398258, at *4 (enjoining defendant from viewing misappropriated documents or using the information they contained).


Id.

Id. at 118-19.

See Cabela’s LLC v. Highby, 362 F. Supp. 3d 208, 223 (D. Del. 2019) (“Federal courts are somewhat divided as to whether a contractual stipulation alone may show irreparable harm.”), aff’d, 801 F. App’x 48 (3d Cir. 2020)

Unif. Trade Secrets Act § 2(a).

E.g., Bimbo Bakeries USA, Inc. v. Botticella, 613 F.3d 102, 111-12 (3d Cir. 2010).


Id. at *13.

Id. The Waymo saga did not end with the civil lawsuit. Although ultimately allowed to assume a position at Uber, the executive was indicted in 2019 for thirty-three criminal counts of trade secret theft under the Economic Espionage Act. See United States v. Levandowski, No. 19-cr-377-LHK-SVK (N.D. Cal. Aug. 15, 2019). On August 4, 2020, the executive was sentenced to eighteen months in prison.


Id.

Id. (following this analysis to award the plaintiff “$207,000.00 in lost profits”).

Rowe, supra note 149, at 162. For a detailed analysis and measurement of price erosion damages, see Salsbury, 735 F. Supp. at 1573.

See Unif. Trade Secrets Act § 3(a).

E.g., GlobeRanger Corp., 836 F.3d at 499-500 (affirming award of $19.7 million based “on an unjust enrichment theory rooted in research and development costs that [the defendant] avoided”).

E.J. Brooks Co., 31 N.Y.3d at 444, 105 N.E.3d at 304, 80 N.Y.S.3d at 165.


Lockheed Martin, 2009 WL 8435667, at *3.
292 Id.
293 Id.
295 Id. at 1317-18.
296 Id. at 1317.
297 Id.
298 Id. (emphasis added).
299 Id. at 1332.
301 E.g., Univ. Computing Co. v. Lykes-Youngstown Corp., 504 F.2d 518, 539 (5th Cir. 1974).
304 Rowe, supra note 231, at 175, 175 n.111 (finding “an average of about $1.1 million in reasonable royalties from bench trials and $434,578.12 from juries”).
306 Brook Shopping Centers, 107 A.D.2d 615, 483 N.Y.S.2d at 1022.
308 Rowe, supra note 231, at 164.