AIGA

Trade Secrets and Nondisclosure Agreements

by Richard Stim

Many design firms use nondisclosure agreements to preserve trade secrets. But simply calling information a trade secret will not make it so. Here's what designers need to know to understand and protect trade secrets.

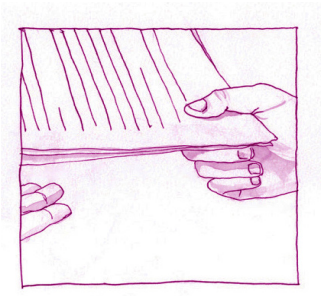
1. What's a trade secret?

A *trade secret* is "any confidential business information which provides an enterprise a competitive edge."[1] In order to acquire legal protection for a trade secret—for example, to stop someone who has stolen a trade secret—the information must:

Be a secret. The information cannot be generally known or ascertainable through legal methods. For example, if a procedure is already known within an industry, it can't be claimed to be a trade secret.[2] Similarly, posting information on the Internet, whether it is details about profit margins[3] in a company that is not publicly traded or lists of blood donors,[4] ends trade secrecy;

Have value. The secret must provide the owner with some competitive advantage in the marketplace. One way of assessing value is to ask whether a business would be damaged if a competitor acquired the information. For example, when a meat packer's secret process for freezing precooked sausage was stolen by a competitor, a jury awarded $10.9 million in lost profits;[5] and

Be treated confidentially. A designer cannot protect information as a trade secret—even using a nondisclosure agreement—unless reasonable precautions are taken to keep the information confidential. In general, a design business is considered to have taken reasonable steps if it uses a sensible system for protecting information—locking its facilities, monitoring visitors, and labeling confidential information as "Confidential."



2. What rights does a trade secret owner have?

Unlike other forms of intellectual property such as patents, copyrights, or trademarks, trade secrecy is basically a do-it-yourself form of protection. You don't register with the government to secure your trade secret, you simply keep the information confidential. Once a trade secret is made available to the public, trade secret protection ends.

Like other forms of intellectual property, a trade secret can be sold (an "assignment"), it can be inherited (a family recipe turned out to be worth millions in 2015)[6] , or it can be exploited on a temporary basis (a "license").

A trade secret owner can stop others from copying, using, and benefiting from its trade secrets in the following situations:

---

1 What is a Trade Secret?.
2 Whitmyer Bros., Inc., v. Doyle.
3 Confederated Tribes v. Johnson.
4 American Red Cross v. Palm Beach Blood Bank, Inc..
5 C&F Packing Co. v. IBP, Inc..
6 Is $3m too much for a family recipe in Singapore?.

Stop an employee (or former employee) from disclosing trade secrets. Under state trade secret laws, employees are automatically bound by a duty of confidentiality and prohibited from improper disclosure of an employer's trade secrets (even without signing a nondisclosure agreement). For example, in 2014, Nike sued three former designers who had left the company, alleging they used Nike's trade secrets for work they did for Adidas. Among the trade secrets allegedly taken were "specific designs, including models of team uniforms and products for the 2016 European Championships, plans for Nike-sponsored athletes, unreleased financial information and projections concerning the company's business and information about Nike's planned launches in the marketplace";[7]

Stop a trade secret thief. Anyone who acquires a trade secret through improper means such as theft, industrial espionage, or bribery can be halted from further use and may even be subject to criminal prosecution. For example, in 2018, an Apple engineer was arrested boarding a plane for China after allegedly downloading Apple documents containing driverless car trade secrets;[8] or

Stop someone who violates a nondisclosure agreement (also known as an "NDA"). An NDA is a contract in which one or both parties agree to maintain trade secrets in confidence. For example, the makers of the video game *Fortnite* sued one of its quality assurance testers for violating his NDA by disclosing features of the game, which were subsequently posted on the Internet.[9]

What Cannot Be Protected as a Trade Secret (or in an NDA)?
The following types of information can never be a trade secret:

Independent discovery/reverse engineering. Anyone who discovers a secret legally and independently—that is, without using illegal means or violating agreements—can use the information without permission. It is not a violation of trade secret law to disassemble and analyze (or "reverse engineer") any lawfully obtained product and determine its trade secret. For example, a designer may use a CAD program to reverse engineer a toy design. Beware, however, some vendor contracts may specifically prohibit reverse engineering a product.

Public domain. Information is public domain if it has been published or publicly displayed or is commonly used within an industry. Even a signed NDA cannot help a company claim trade secret

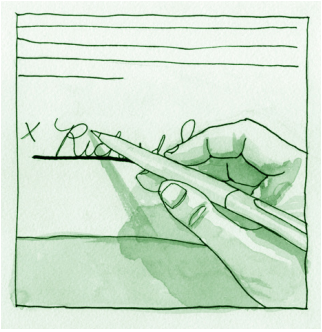
7 Nike sues former designers.
8 Former Apple Engineer Reportedly Charged With Stealing Autonomous Car Secrets.
9 Epic Games sued the leaker of Fortnite comet strike location.

rights if the information is public domain. For example, a tool company hired a designer to create a sealed bearing pack for a motor. After the designer created a similar device for a rival business, the tool company sued the designer and was awarded $1.3 million dollars for trade secret theft. But in 2017, the designer dodged a bullet when the case[10] was reversed by the Colorado Court of Appeals and the designer was absolved of liability. The court held that the design was public domain because it had been known in the industry for decades.

Published patent applications. To obtain a patent on an invention, the inventor must fully describe the invention in the patent application. The U.S. Patent and Trademark Office (USPTO) treats patent applications as confidential, making it possible to apply for a patent and still maintain the underlying information as a trade secret, at least for the first 18 months of the application period.

Unless the applicant files a Non-publication Request at the time of filing and doesn't file for a patent outside the United States, the USPTO will publish the application within 18 months of the filing date. When a patent application is published by the USPTO, all of the secret information becomes public and the trade secret status of the application is lost.

Illegal secrets/illegal contracts. Information won't be protected if it contributes to illegal activity—for example, information used for insider trading. Similarly, information won't be shielded if the NDA was executed for an illegal purpose. For example, an NDA used to hush a scandal during an election campaign might be invalid if it violates campaign financing laws.[11]



3. How do you fulfill secrecy obligations?

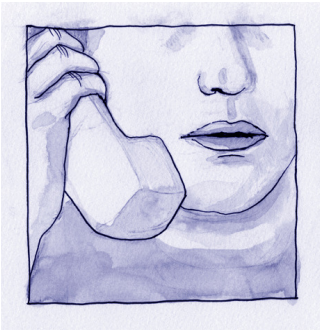
When you conduct a Google search on something, you are using a trade secret—the algorithm that powers Google's search engine and ranks the results.[12] Google works hard to maintain secrecy for its code and employs more than 500 full-time security people in its software engineering division.[13] The company routinely refuses legal demands to view the code made by U.S. regulators and foreign governments.[14]

Although you should take reasonable precautions to protect any information you or your clients regard as a trade secret, you don't have to turn your design

10 Court Overturns $1.3 Million Trade Secret Award Because Design Isn't Secret.
11 Trump and NDAs.
12 Google Schools Its Algorithm.
13 Google Has a Strong Security Culture.
14 Good luck in making Google reveal its algorithm.

firm into an armed camp to do so. Sensible precautions include, for example, marking documents containing trade secrets "Confidential," locking away trade secret materials after business hours, maintaining computer security, and limiting access to secrets to people with a reasonable need to know.

But the best way to establish and protect trade secrets is through the use of nondisclosure agreements. This is because courts have repeatedly said that the use of nondisclosure agreements is the most important way to maintain the secrecy of confidential information.



4. Designers and NDAs

In 1980, IBM needed an operating system for its new personal computers. A California company would not sign IBM's nondisclosure agreement, so IBM contacted Bill Gates who had a rival operating system. Gates signed the NDA, licensed MS-DOS to IBM, and Microsoft was launched.[15] Signing an NDA doesn't, by itself, assure the signer a future as a billionaire, but it does provide reassurance to a business that wants to hire you (as IBM demonstrated). If a trade secret is disclosed in violation of the NDA, the trade secret owner can file a lawsuit, obtain a court order to stop further use of the trade secret, and recover money for the damage caused by the disclosure.

A staff designer in a design firm usually executes two types of NDAs: a client NDA that places disclosure limitations on client information, and an employee NDA that protects the design firm. Although state laws require employees to maintain trade secrets, all employees of a design firm who come into contact with the designer's and the client's trade secrets should sign nondisclosure agreements.

As for client NDAs, one of the major considerations is whether the design firm will be disclosing any of its own secrets to the client. If so, the NDA should be mutual ("bilateral") so that both designer and client are obligated to maintain secrecy. If the designer won't be disclosing secrets, then the agreement can be one-way ("unilateral").

NOTE: *The AIGA Standard Form of Agreement for Design Services* at Section M 7.1 in the supplement for motion design includes a mutual trade secret provision.[16]

Key Elements of an NDA

Sometimes NDAs are stand-alone agreements and sometimes the provisions are incorporated into another agreement, for example, a contractor agreement or a work order. Regardless of where they are found, the key elements in an NDA include:

15 Did Bill Gates Steal the Heart of DOS?

16 AIGA Standard Form of Agreement for Design Services.

Definition of trade secrets. Every nondisclosure agreement starts with a definition of the trade secrets, often referred to as "Confidential Information." There are three common strategies for defining confidential information. What's best? That depends on your secrets and how you disclose them.

DEFINITION 1: LISTING TRADE SECRET CATEGORIES.
If your company focuses on several categories of secret information, for example, computer code, sales information, and marketing plans, a list approach will work with employees and contractors. This is the most common strategy and it's the approach taken by AIGA in its model agreement (see sidebar).

DEFINITION 2: LABELING THE CONFIDENTIAL INFORMATION.
In this definition, the trade secret owner has the obligation to label written trade secrets as "Confidential"—that is, if it is not labeled then it cannot be claimed as a trade secret. In the case of oral disclosures, the disclosing party provides written confirmation that a trade secret was disclosed. Here is an example of what the provision would look like:

> *Definition of Confidential Information (Written or Oral). For purposes of this Agreement, "Confidential Information" includes all information or material that has or could have commercial value or other utility in the business in which Disclosing Party is engaged. If Confidential Information is in written form, the Disclosing Party shall label or stamp the materials with the word "Confidential" or some similar warning. If Confidential Information is transmitted orally, the Disclosing Party shall promptly provide a writing indicating that such oral communication constituted Confidential Information.*

DEFINITION 3: SPECIFICALLY DESCRIBING THE SECRETS.
If confidential information consists of one or two specific pieces of information—for example, a unique modification to a CAD program—the parties may define it specifically (provided they don't reveal the secret in the agreement). Here is an example of that type of definition:

> *Definition of Confidential Information. The following constitutes Confidential Information: a method for modifying a CAD program to track preparation of design elements, and related algorithms and software code.*

Excluding information that is not confidential. You cannot prohibit someone from disclosing information that is publicly known, legitimately acquired from another source, or developed by the other party before meeting you. These legal exceptions exist with or without an agreement, but they are commonly included in a contract to make it clear to everyone that such information is not considered a trade secret.

AIGA Trade Secret Definition.

§ M 7.1 - Definition. Each Party's "Trade Secrets" shall mean a Party's proprietary property, including information, ideas, patterns, compilations, data, lists, documents, memoranda, processes, programs, devices, methods, techniques, formulas or improvements, whether or not patentable, which meets the following criteria:

a. the other Party becomes aware of the property as a consequence of performing its obligations under this Agreement;
b. the property has independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use, and
c. the Party has made reasonable efforts under the circumstances to maintain the secrecy of the property. Each Party acknowledges that the other Party's' Trade Secrets are Confidential Information subject to the Confidentiality provisions of this Agreement.

Duty to keep information confidential. The heart of a nondisclosure agreement is a statement establishing a confidential relationship between the parties. The statement sets out the duty of the party receiving the secret (the "receiving party") to maintain the information in confidence and to limit its use. In some cases, the trade secret owner may want to impose additional requirements. For example, if your secrets consist of software, your NDA may contain a prohibition against reverse engineering, decompiling, or disassembling the software. This prohibits the receiving party (the user of licensed software) from learning more about the trade secrets. You may also insist on the return of all trade secret materials that you furnished under the agreement. Clients may have more specific limitations. For example, a designer may be prohibited from including any client work in the designer's public-facing portfolio or the designer's résumé. In many cases, a client or employer may want the designer to maintain secrecy for a period following termination—that is, to not discuss the project for several years after the work has ended.[17]

Duration. How long does the duty of confidentiality last? There are three common approaches: an indefinite period that terminates when the information is no longer a trade secret, a fixed period of time, or a combination of the two. The time period is often an issue of negotiation. Trade secret owners usually want an open period with no limits; receiving parties want a short period. For employee and contractor agreements, the term is often unlimited or ends only when the trade secret becomes public knowledge. Five years is a common length in nondisclosure agreements that involve business negotiations and product submissions, although some companies prefer three or two years.

17 The Rise and Fall of Design Within Reach.

Miscellaneous Provisions in an NDA

An NDA, like most agreements, includes miscellaneous provisions (sometimes known as "boilerplate" language) that are usually located at the end. These provisions are important and can affect how disputes are resolved and how a court enforces the contract. Below are four of the more important provisions.

Injunctive relief. An injunction is a court order directing a person to do (or stop doing) something. If someone violated your NDA, you would want a court order directing that person to stop using your secrets. To get an injunction, you must demonstrate to the court that you have suffered or will suffer irreparable harm as a result of the unauthorized use of your secrets. Irreparable harm is harm that can't be compensated for later by money. Proving that in court is expensive and time-consuming. In order to cut through some of that legal work, some nondisclosure agreements include a provision in which the receiving party agrees that the harm caused by a breach is irreparable, so you will have less to prove if and when you seek a court order. This provision only makes it easier to obtain an injunction; by itself, it will not compel a judge to order an injunction.

Indemnity. Some NDAs require the receiving party to pay for all damages (lost profits, attorney fees, or other expenses) incurred by the other party as a result of the receiving party's breach of the nondisclosure agreement. This obligation is known as indemnification. Leaving out the indemnity provision does not prevent the owner of a trade secret from suing and collecting damages for a breach (contract law holds the receiving party responsible for a breach), but the clause makes it easier to claim damages.

Attorney fees clause. If you don't include an attorney fees clause in your agreement, a judge may (in most states) order the award of attorney fees in cases where the theft of the trade secret was willful and malicious. It's up to the judge, which makes things unpredictable. You are far better off using an attorney fees provision. Because lawyers are so expensive, having an attorney fee provision—that is, having each side afraid it will get stuck paying someone's attorney fees—can prove crucial to ending a dispute.

Jurisdiction. The purpose of adding a jurisdiction provision to an NDA is to get each party to consent in advance to jurisdiction in one county or state and to give up the right to sue or be sued anywhere else. This may seem like a trivial issue at the time you are negotiating an agreement, but it will be a major issue if there is ever a dispute.

Employee NDAs: A Required Notice

Under the Defend Trade Secrets Act (DTSA) (discussed below), employees, independent contractors, and consultants are shielded from liability for disclosing trade secrets for certain whistleblowing activities. These activities include disclosure of a trade secret:

« *In confidence to a government official or to an attorney for the purpose of reporting or investigating illegal activity,* and
« *In legal documents under seal (not part of the public record) in a judicial proceeding.*

Employers are required to include a notice of immunity "in any contract or agreement with an employee that governs the use of a trade secret or other confidential information." Including this notice benefits the employee—it puts the employee on notice about whistleblowing and trade secrets—and the employer—by including the provision, the employer who prevails in a lawsuit is permitted to recover exemplary (double) damages and attorney fees from the employee or contractor. The failure to include the provision does not prevent filing in federal court under the DTSA. A sample NDA provision would include the following language:

Notice of Immunity from Liability. An individual shall not be held criminally or civilly liable under any federal or state trade secret law for the disclosure of a trade secret that 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. An individual who files a lawsuit for retaliation by an employer for reporting a suspected violation of law may disclose the trade secret to the attorney of the individual and use the trade secret information in the court proceeding, if the individual (i) files any document containing the trade secret under seal; and (ii) does not disclose the trade secret, except pursuant to court order.

5. Trade secret laws: when secrets are stolen

A client or employer, angered over a designer's unauthorized disclosure of a trade secret, can use the law to sue and recover financial payments from the designer. For example, J. Crew sued[18] a former senior designer when management learned that before leaving the company to work for a competitor, he e-mailed confidential J. Crew information to his personal e-mail account. These documents included product design specifications and measurements,

18 J. Crew Group v. Fenton.

the production development calendar, contact information for key manufacturing resources, and design inspirations.[19]

Trade secrets are protected by state and federal law. Every state has enacted a law prohibiting theft or disclosure of trade secrets. Most of these laws are derived from the Uniform Trade Secrets Act (UTSA), a model law drafted by legal scholars. Forty-nine states and the District of Columbia have trade secret laws adopted from the UTSA (New York, which has its own trade secret law, has not adopted it).

The Defend Trade Secrets Act (DTSA), signed into law in May 2016, "federalizes" trade secret law by providing a procedure for trade secret owners to file civil lawsuits in federal court. Any company possessing a trade secret that is used in interstate or foreign commerce can take advantage of the provisions of the DTSA. Prior to the DTSA, trade secret owners could only bring civil lawsuits in state courts, under state laws based on the UTSA. In many important ways the DTSA and state laws based on the UTSA are similar but the DTSA may be more favorable to trade secret owners because it provides access to federal courts and it provides for seizing trade secrets without giving any notice to the defendant, an unprecedented leap from the notice requirements of state laws based on the UTSA.

Criminal Theft

A designer may also, in rare cases, be subject to criminal prosecution and imprisonment. For example, a judge recommended criminal prosecution of an autonomous vehicle engineer who allegedly stole secrets from Google's autonomous vehicle company, Waymo.[20] In a 2007 case,[21] two ex-Coca-Cola employees were sentenced to eight and five-year prison sentences, for trying to sell Coke's secrets to Pepsi (Pepsi blew the whistle on the thieves).

Intentional theft of trade secrets can constitute a crime under both federal and state law. The most significant federal law dealing with trade secret theft is the Economic Espionage Act of 1996 (EEA). The act gives the U.S. Attorney General sweeping powers to prosecute any person or company involved in trade secret misappropriation.

The EEA punishes intentional stealing, copying, or receiving of trade secrets "related to or included in a product that is produced for or placed in interstate commerce." (18 U.S.C. 1832.) Penalties for violations are severe: Individuals may be fined up to $500,000 and corporations up to $5 million. A violator may also be sent to prison for up to 10 years. If the theft is performed on behalf of a foreign

19 J. Crew Sues Former Designer for Alleged Trade Secrets Violation.
20 Steal A Trade Secret, Go To Jail?
21 Two ex-Coke workers sentenced in Pepsi plot deal.

government or agent, the corporate fines can double and jail time may increase to 15 years. (18 U.S.C. 1831.) In addition, the property used and proceeds derived from the theft can be seized and sold by the government. (18 U.S.C. 1831, 1834.)

Several states have also enacted laws making trade secret infringement a crime. For example, in California it is a crime to acquire, disclose, or use trade secrets without authorization. Violators may be fined up to $5,000, sentenced to up to one year in jail, or both. (Cal. Penal Code Section 499c.)

One Final Note

A philosopher[22] once wrote, "When a secret is revealed, it is the fault of the man who confided it." In other words, there's more to protecting secrets than labeling information "Confidential" and signing a nondisclosure agreement. An NDA can provide you with benefits and advantages when going after thieves, but no matter how carefully it is drafted it will not shield you from someone determined to commit dishonest acts. The key to successfully maintaining trade secrecy is to combine the legal rules discussed in this article with common sense and vigilance.

ABOUT THE AUTHOR: Attorney Richard Stim specializes in small business, copyright, patent, and trademark issues. He practices law in Sausalito and has represented photographers, software developers, craftspeople, publishers, musicians, and toy designers. He is the author of many books, including *Music Law: How to Run Your Band's Business*, *Patent, Copyright & Trademark: An Intellectual Property Desk Reference*, and *Profit From Your Idea*.

ABOUT THE ILLUSTRATOR: Sasha Stim-Fogel is an artist living in Beacon, New York.

22 Jean de la Bruyere.