PREPARED BY

GalkinLaw

internet law · new media law · technology law

THE ESSENTIAL

TRADE SECRET PROTECTION GUIDE

GOT QUESTIONS ABOUT TRADE SECRETS?

CONTACT US FOR A FREE CONSULTATION AT

www.galkinlaw.com or inquiries@galkinlaw.com

THE ESSENTIAL

TRADE SECRET PROTECTION GUIDE

PREPARED BY

GalkinLaw

internet law · new media law · technology law

CONTENTS

Introduction to Trade Secret Protection

Trade secret protection is a form of intellectual property. Other forms of intellectual property include copyrights, patents, and trademarks. Trade secret protection applies to information that is not generally known and that has commercial value to the possessor of that information. Information typically protected as trade secrets includes business plans and opportunities, inventions, data, methods, formulas, software, customer lists, product and marketing plans, and supplier lists.

Trade secret protection is the only way under U.S. law to protect a non-patented or non-patentable idea. Other forms of intellectual property do not require a persistant effort to maintain the value of the intellectual property. However, the availability of trade secret protection requires that the possessor of that information proactively and diligently keep that information secret. A failure to do so will result in the loss of trade secret protection. Another difference between trade secrets and other forms of intellectual property is that trade secrets can be stolen, for instance when hacked or removed by an employee, and can also be "destroyed" by public disclosure. Other forms of intellectual property cannot be stolen in this manner.

In order to enforce a trade secret, the owner must show that he has taken reasonable steps to protect the trade secret from disclosure. One of the primary ways necessary to show that such reasonable steps have been taken is to enter into a non-disclosure agreement with the recipient of the information. However, various additional steps need to be taken as well, which will be discussed below.

Terminology: ***Non-disclosure agreements may also be referred to as confidentiality agreements, trade secrets agreements or NDAs. In this Guide, non-disclosure agreements will be referred to as NDAs. The terms trade secrets and confidential information are often used interchangeably, though there are some distinctions between these terms. In this Guide we will use the term trade secrets, except where confidential information is specifically discussed. In this Guide, the party disclosing the trade secret is referred to as "the disclosing party" and the party receiving the trade secret is referred to as "the receiving party."***

What is the legal basis for trade secret protection?

In the United States, trade secrets are protected under the laws of each state, the Uniform Trade Section Act (UTSA) (which has been adopted in all states except New York, North Carolina and Massachusetts), and under federal law under the Defend Trade Secrets Act.

What is a non-disclosure agreement or NDA?

Non-disclosure agreements may also be referred to as NDAs, confidentiality agreements, or trade secrets agreements – they are all the same thing. In this Guide we will be referring to this type of document as an NDA.

An NDA is a written agreement between parties where they define trade secret information that may be disclosed between the parties and prohibits each party from (1) from further disclosing the trade secret information of the other party to anyone else without the disclosing party's permission and (2) using that trade secret information for any purpose not approved by the disclosing party. NDAs are usually entered into between two parties, but there may be more than two parties when necessary. The parties entering into an NDA can be individuals or businesses.

In order to restrict a receiving party from disclosing or using trade secret information, the possessor of that information must be able to demonstrate to a court that a reasonable effort was made to maintain the secrecy of the information. An NDA acts as a key component to demonstrate that this effort was reasonably made.

An NDA is not just a form. An NDA needs to be tailored to the parties' needs and expectations. NDAs are only enforceable through litigation. NDAs provide an imperfect protection. Therefore, it is also important to be careful when choosing who to disclose to.

What are the different types of NDAs?

NDAs can be one-sided (unilateral) or two-sided (mutual). A one-sided NDA is used when only one party will be disclosing information and a two-sided NDA will be used when both parties will be disclosing information. For example, an NDA for an employee will always be one-sided, as only the employer is disclosing trade secret information and if the employee develops trade secret information, that will be protected under the NDA as trade secret information owned by the employer. Whereas, where business relationships are being established a two-sided NDA will usually be used.

There are situations where it is not clear whether a one-sided or two-sided NDA is more appropriate, like for a consultant. A consultant may act like an employee or a consultant may bring to a project the consultant's own unique tools, procedures and skills, which the consultant will want to protect under an NDA. Under such situations the parties need to determine the most appropriate NDA to use.

There is always a risk of liability when a party receives trade secret information from another party. Therefore, a one-sided NDA is a safer bet for the disclosing party. On the other hand, mutual NDAs are usually drafted in a fairer manner, because the terms equally apply to both parties. Accordingly, an initial decision needs to be made as to whether a one-sided or two-sided NDA is more appropriate under the circumstances.

Following is a brief description of common situations that will call for somewhat different terms NDAs to be used:

Potential Business Partner:	This is one of the most common circumstances for an NDA. Two parties are considering entering into a business relationship and want to have open discussions. This will usually be a mutual NDA. It is beneficial to mention in the NDA the type of relationship being considered and that neither party has any obligation to actually enter into that relationship.
Employee:	NDAs for employees are one-sided. Additionally, all trade secret information created by the employee during that employee's employment will be owned by the employer.
Contractor:	NDAs for contractors may be one-sided or two-sided. The preference by a customer would be a one-sided NDA that protects the customer's information and information developed by the consultant. However, often consultants bring proprietary tools and procedures and will insist on a two-sided NDA.
Potential Acquisition/Investor:	NDAs for a potential acquisition/investor can be one-sided or two-sided. The strong preference from the target company's perspective would be a one-sided NDA. However, the potential acquirer/investor may

	be coming with some market intelligence that it wants protected. A potential acquirer/investor will often get deep access to trade secret information. Therefore, it may be necessary to limit disclosure to named individuals and have strong requirements and restrictions on copying information, and regarding return and destruction of trade secret information if no acquisition/investment occurs.
Invention Disclosure:	These NDAs can be tricky, especially because the invention usually relates to the receiving party's business. The inventor does not want to disclose the idea until an NDA is signed. The receiving party does not want to be bound by restrictions on a new invention that might restrict the operation of their business. One way of handling this is for the NDA to provide for a 2-stage disclosure. First, limited information is disclosed and the receiving party can then decide whether it wants to receive more information. If it does, then the parties can sign an Exhibit to the NDA specifying, in general, the invention. The inventor should try to have this be a one-sided NDA.
Beta Tester NDA:	Often websites, software and other products have a pre-release stage where a limited universe of users is asked to test out the service or product. Since the service or product are not out on the market, the business will want details regarding the service or product to remain confidential until public launch. This will be a one-sided NDA.
Audit NDA:	Many agreements provide that one party may audit the other. Often the audit is done by independent third parties. It is important that the third party auditor sign an NDA because the third party will be having access to very sensitive internal information.
Top Secret NDA:	Sometimes information is top secret, like source code to a company's primary software protect. If source

code needs to be disclosed, then heighten protections may be required, like (1) disclosure only to named individuals, (2) no duplication, (3) storage in location subject to stated security requirements, and (4) right to audit compliance with these requirements.

What type of information are NDAs used to protect?

In order to be protected by an NDA, information must be either a trade secret or confidential information. Trade secrets were previously defined as information that is not generally known and that has commercial value to the possessor of that information. There is other information that does not qualify as a trade secret, but could still be protected by an NDA as confidential information. For instance, businesses do not want information in their financial statements to be disclosed. This information is not generally known. However, it may not provide a commercial advantage to the business. This information could be restricted as confidential information under an NDA. It is often not clear whether information is a trade secret or merely confidential information. So both types of information are usually grouped together in an NDA under the definition of Confidential Information.

The types of trade secret or confidential information that can be disclosed can include intellectual property, technical information, business, and commercial information.

Here are some examples of trade secrets or confidential information:

Business/Commercial:	Customer databases, contact lists, prospect lists, mailing lists, supplier lists, programmers lists, product development and acquisition plans, cost and profit margin information, contract bids, and business strategy documents.
Technical:	Software, source code, procedures, techniques, data analysis methods, graphics display techniques, encryption and compression techniques, and optimization methods, etc.

What type of information will an NDA not protect?

An NDA cannot make a trade secret something that is not a secret. So information that falls into one of the following categories will not be protected from disclosure and use:

- Information which is or becomes a matter of public knowledge through no fault of or action by the receiving party
- Information that was in the receiving party's possession prior to disclosure by the disclosing party
- Information which, subsequent to disclosure, is rightfully obtained by the receiving party from a third party who is lawfully in possession of such information without restriction
- Information that is independently developed by the receiving party without resort to the disclosing party's information

What legally qualifies as trade secret information?

The standard definition of a trade secret is (from the Uniform Trade Secrets Act):

> Information, including a formula, pattern, compilation, program, device, method, technique, or process, that:
>
> (a) the information in question is not generally known to the public;
>
> (b) the non-public nature of the information confers an economic benefit; and
>
> (c) the owner of the information takes reasonable steps to protect the information from public disclosure.

Classic examples of trade secrets that meet the above definitions are the recipes for Coca Cola or KFC chicken or the process used to make the "nooks and crannies" in Thomas English Muffins.

Accordingly, the following 3 tests must be passed in order to qualify information as a trade secret:

Not generally known or readily ascertainable

If information is generally known, then it is not a secret, and certainly not a trade secret, even if the receiving party is not aware of the information. For instance, you are aware of a certain logistics software application that your competitor is not aware of and that application will give you a competitive advantage. Since the logistics program is publicly advertised and distributed, it cannot be a trade secret. Additionally, even if

information is not generally known, but it is ascertainable without exerting great effort, then the information also does not qualify as a trade secret. For instance, even though customer lists often qualify as trade secrets, but your industry has a relatively small number of prospective customers, then your customer list may not qualify as a trade secret because a list of all prospects, which can be compiled with minimal effort, may substantially resemble your customer list. Additionally, if the unique aspects of your product can be reverse engineered by someone with proper skill who legitimately obtains your product, then those unique aspects would not qualify as a trade secret.

Information or techniques generally known by a skilled person in that industry, though taught to the employee at great expense, would not qualify as trade secret.

If someone publicly reveals your trade secrets in violation of your NDA, then that information can no longer be treated as a trade secret, though you will be able to take legal action against the unauthorized disclosure. This is why if you think an unauthorized disclosure may have occurred or might occur, you need to take legal action as quickly as possible to prevent or limit the disclosure so that you do not lose trade secret protection over that information.

Has commercial value

Information, though not known generally, and difficult to ascertain, but has little or no economic value will not be treated as a trade secret. For instance, a secret recipe for a product that has no economic value, would not qualify as a trade secret.

Efforts to maintain confidentiality

In order to maintain trade secret protection, you must make reasonable efforts to keep the information secret.

It is not called a trade secret for nothing! When you have a personal issue that you want to keep secret, you do not go around telling everybody about it, and you certainly do not tell Aunt Nellie who you know loves telling "secrets" to the family. In business it is the same thing. If you have a valuable secret, then you do not go telling your great idea to everyone you meet. That would show that you do not treat it like a secret, and then it will lose its trade secret status (e.g., no legal protection). Therefore, all disclosures of trade secret information should be subject to an NDA (whether to third parties or to employees/contractors) as a demonstration of your effort to maintain the secrecy of the information.

Here are some examples of failures to make reasonable efforts to maintain the confidentiality of an idea:

- Discussing the idea with people without having them expressly agree to keep it confidential (through an oral commitment or having them sign an NDA).
- Creating a business plan and distributing the plan to multiple people without obtaining a commitment to maintain confidentiality.
- Leaving papers describing a product roadmap on a desk or table in an office where it is accessible by people not bound by non-disclosure obligations.
- Having business plans, or customer lists, etc. accessible over a network (or the Internet!) or in a file cabinet which is accessible to people not bound by non-disclosure obligations

Here are some examples of additional actions that demonstrate a desire to maintain secrecy:

1. Premises Security: Restricted access to premises, codes on entry doors, issuing passes to visitors, etc.
2. Computer/Network Security: Implementing what is considered reasonable computer security in the industry, like strong passwords that are changed regularly, firewalls, limiting laptop access, limiting data that can be removed on mobile devices, and regular network monitoring.
3. Encryption: Encryption of sensitive data when in storage or when transferred.
4. Limited to "Need to Know": Limiting access to data only to those personnel with a need to know the data.

What is considered *reasonable* will vary with the circumstances. Top secret information requires higher measures than a simple software protect. Large corporations require more procedures than a small company. Different industries may have different standards of protection that are commonly used.

Can you have an oral NDA or an oral obligation to maintain confidentiality?

You cannot have an oral NDA, because, by definition, an NDA is an agreement in writing. However, it is possible to have circumstances where information is disclosed and the receiving party understood that the information was meant to be kept confidential. The difficulty will be in proving that the receiving party was informed or should have reasonably understood that a non-disclosure obligation was applicable to the disclosure of the information. What is more, since NDAs are so common, a court is likely to view the failure to have an NDA signed as

evidence that the disclosing party was not making reasonable efforts to protect the trade secret information. So always use an NDA!

What to do if you want to make sure that you DON'T receive trade secrets?

Some companies want to make sure that they do not receive trade secret information, unless they expressly allow it. This is accomplished by having the parties sign a "non-NDA." This non-NDA basically says that nothing that is disclosed is confidential unless that information is specified in an NDA. A non-NDA is not common, but can be useful for transactions where competitive information might be disclosed and the parties do not want to chance a law suit by inadvertently using that information.

Should an NDA be superseded by a formal agreement?

After signing an NDA, often the parties enter into a formal agreement documenting a transaction or business relationship. These agreements usually contain non-disclosure provisions. The question that arises is whether the NDA should be superseded by the confidentiality provisions of the formal agreement. The formal agreement should either expressly supersede the NDA or incorporate its terms as a replacement for the agreement's confidentiality terms. However, there should not be two separate and possibly conflicting non-disclosure provisions. An NDA that was already negotiated is easy to incorporate by reference into the formal agreement, and would often have more robust terms than the agreement, but it is important to review the terms of the NDA to verify that it will survive for at least the term of the formal agreement. If the NDA is not incorporated, then it is important to consider whether the limitation of liability provisions will or will not apply to breaches of confidentiality restrictions in the formal agreement. This is because in an NDA, breaches of confidentiality are usually subject to unlimited liability, and you may or may not want that unlimited liability to continue to apply under the agreement.

When do you sign an NDA?

The earlier you sign an NDA the better. Sometimes people are reluctant to ask to have an NDA signed because they think this will appear to be too pushy or formal. That should not be a concern when trade secrets are involved. In all likelihood, requesting that the parties sign an NDA will make the requesting party appear professional and serious about the discussions. What often happens is that if the parties do not sign an NDA early, then they forget to sign one when the discussions get more serious.

If an NDA was not signed early, then the NDA that is signed later can state that all earlier information disclosed is also considered to be trade secrets.

Should all employees and contractors sign an NDA?

Absolutely, all employees and contractors should sign NDAs. Even low level employees and contractors may have access to trade secret information that can then be disclosed to competitors or used to the detriment of your company. Signing NDAs should be part of every company's onboarding process for all employees and contractors.

What are the different intellectual property rights used to protect ideas and inventions other than trade secret protection?

There are 3 primary ways of protecting valuable information, ideas or inventions: (1) trade secret protection, (2) copyright protection and (3) patent protection. Each of these protections are distinct but may at times be used together.

Trade secret protection is the subject of this Guide and has already been discussed in detail. However, it is important to be aware of the other available protections in case you can take advantage of them.

Patents protect inventions and processes that are novel and non-obvious. Mere ideas (like the idea to create a niche social network) is not protectable by a patent regardless of how valuable the idea might be. However, there may be some functional features of the niche social network that might be patentable, but not the general idea itself. One of the early patents granted for website functionality was the "one-click" checkout process for Amazon purchases.

The patent process is rather expensive ($5,000 and up – possibly way up) and long (let's say between 2 and 3 years). So, while patent protection is the strongest protection you can get, you will need a qualifying invention, as well as the time and money. You may have a choice to either patent an invention or maintain trade secret protection. Both protections cannot be available for a single invention because during the patent applicable process (usually after about 18 months), the details of the patent will be made public – so no trade secret protection could then be maintained.

PROS AND CONS OF PATENTS V. TRADE SECRETS		
	Patent	**Trade Secret**
Term of Protection	20 years	Forever or until no longer qualifying as a trade secret
Strength of Protection	Very strong	Depends upon level of secrecy maintained
Cost	$5,000 and up	No charge
Timing to obtain protection	2 to 3 years before a patent will issue	Immediate
Risks	Disclose invention during application process, then not get the patent (and be left with no trade secret and no patent protection) or get issued a much narrower and less valuable patent than was originally expected.	Someone could receive a patent that blocks use of your trade secret.

Copyright protects the tangible expression of ideas. Think of a video, a book or music. Copyright will protect the way ideas are expressed but not the ideas themselves. Someone can write a book on gardening methods, and the photos and wording used to describe the gardening methods will be protected by copyright. However, the methods described are free to be used by anyone. Copyright is a strong protection for the manner of expression, applies immediately upon creation of the work, and is inexpensive to obtain.

So if the item you want to protect might be covered by a patent, then you should have a patent attorney review the idea and make an initial assessment. If the idea is already expressed in a tangible form like a book, then you can enjoy copyright protection. However, if the idea or ideas do not fall into any one of those categories, then trade secret protection is going to be your best bet.

As opposed to patent and copyrights, which are protected under U.S. federal law, trade secrets are protected under both state law (including for all states, except New York, North Carolina and Massachusetts, under the Uniform Trade Secrets Act) and federal law (the Defend Trade Secrets Act adopted in 2016).

What are the ways confidential information can be leaked?

Let me count the ways! You can just use your imagination on this one. But here are some examples to get your imagination flowing: conversations in elevators or restaurants, presentations at conferences, published papers, company websites, social media, disgruntled employees, public filings, third party vendor relationships, etc.

If broadly leaked, protection is lost. If there is only a limited disclosure, then not.

Know your circumstances and evaluate the weak spots. Be proactive to avoid trade secret leaks.

What is the length of trade secret protection?

Trade secrets will remain protected under the law as long as they remain secret and valuable. How long has the Coca Cola recipe been a trade secret? Well over 100 years!

Can more than one person have the same trade secret?

It is possible for more than one person to possess the same trade secret. Let's say there is a unique method for making Swiss cheese. Two master cheese makers may have come up with the same idea independently and have kept it as a trade secret. However, if one discloses it publicly, the other cheese maker will automatically lose trade secret protection.

What are the key provisions in an NDA?

An NDA is not just a "form" document. NDAs have many clauses which should be tailored to address the specific circumstances around the disclosure. Small variations in provisions can make a big difference on trade secret protection and liability for a breach of confidentiality.

What follows is a brief description of some of the various clauses and issues to consider:

Identifying the parties

It is important to determine who should be the correct parties listed in your NDA. For instance, should the parties be individuals or businesses? In any case, you should obtain the correct legal name for each party. For a business that will usually mean that the name ends with "Inc." or "LLC." It is also important to obtain correct current addresses for each party. This is important because this more specifically identifies the parties, but

also because if a party needs to send notice to the other party, the stated address would be used.

Statement of purpose

An NDA should state the purpose of the disclosure. For instance, to discuss a potential business relationship, to perform due diligence for a potential investment, etc. The stated purpose will define the scope within which each party can use the disclosed information of the other party.

Definition of confidential information

There are several approaches to the definition of confidential information: (1) general description, (2) specific description, and (3) marked documentation only.

- General Description – This is easy to draft and is broad, but it is vague and difficult to apply unless other measures are taken to clarify what the confidential information is. The issue will be what was intended to be covered – and some courts may find it too broad to be enforced at all. Even with the risks, this still remains the most common approach.
- Specific Description – This approach is used when the disclosure is focused on a single idea or technology.
- Both General and Specific Description - This is the best approach where you cover all bases.
- Marked Items - Some NDAs limit confidential information to information that is in documents marked "Confidential" or written summaries of confidential conversations. This approach has the benefit of removing all doubt as to what information is intended to be confidential. However, the risk is that a party fails to mark a document or summarize a conversation, which then makes that disclosed information not confidential.

Exceptions to confidential information

Standard exclusions to the definition of confidential information are (1) information that is in the public domain, (2) information that was in the receiving party's possession before the disclosure or was rightly received from a permitted source after the disclosure, (3) information that is independently developed, and (4) court ordered or legally required disclosure. It is usually beneficial to provide that a party that wants to rely on one of these exclusions be required to provide documentary evidence to the support their claim.

Prohibits disclosure

An NDA prohibits disclosure of trade secret information. However, there is usually a list of the types of disclosures that are permitted, such as to employees, consultants, financial and legal advisers, and to affiliates. The agreement should require as a condition to these disclosures that the disclosures be on a need to know basis and that the recipients have been made aware of the confidential nature of the information and are bound by appropriate non-disclosure restrictions.

Prohibits use

Just like an NDA prohibits unauthorized disclosures, an NDA also needs to prohibit unauthorized use of the trade secret information. Some NDAs leave this out. It may be an oversight or it might be intentional, but it greatly weakens the protection of the trade secrets. Use should be limited to stated purpose.

Prohibit reverse engineering

A product might not be a trade secret, but how the product works on the backend might be. Therefore, if a recipient of a test product can reverse engineer it to reveal the secrets on the backend, then that reverse engineering needs to be specifically prohibited. A classic situation is software. Software might be widely distributed, but the source code is not. If a recipient can reverse engineer the source code, then the source code will no longer be a trade secret. Therefore, reverse engineering needs to be prohibited.

Ownership retention

It is important that an NDA clearly states that the NDA does not transfer any ownership in disclosed information, not even in the form of a license.

Residuals clause

A residuals clause allows each party to use information disclosed that is retained in a receiving party's unaided memory. This is a clause that should only be included after careful consideration because it can act as a major exception to the restrictive conditions.

Warranty disclaimer

An NDA should exclude any warranties as to the accuracy or completeness of information disclosed so that if a receiving party relies on that information and it is inaccurate, the disclosing party is not responsible.

Return/destruction of information

At the end of a term of an NDA, or upon an earlier request, all trade secret information should be returned or destroyed, and this should be certified as completed by management of the receiving party.

Liquidated damages

Some NDAs impose a specific monetary fine for a breach. The problem is that many states will not enforce the clause and it may actually impair ability to get an injunction because a court will only grant an injunction if there is no adequate remedy at law available. The stated damage amount, if enforceable, implies that there is a remedy at law – i.e., the stated damage amount. However, the upside is the fear factor benefit of such a clause.

Term of agreement

The term of an NDA has 2 meanings: (1) the length of time that disclosures are covered by the NDA, and (2) the length of time disclosed information remains subject to the NDA. Usually, even upon the termination of an NDA, information should remain subject to the restrictions of the NDA indefinitely or until the information no longer qualifies as a trade secret. However, some businesses prefer that confidentiality restrictions be limited in time (e.g., 3 years). Various considerations might affect how the term provision is drafted.

Equitable relief

An NDA should state that each party recognizes that damages might not be a sufficient remedy for a breach of the NDA and equitable relief or an injunction should be available. Such a clause can make it more likely that a court will grant an injunction to prevent a disclosure or continued disclosure.

Attorney fees

Under most state laws, attorney's fees will not be awarded to the party prevailing in a legal action unless stated in the applicable agreement. So, such a clause should be considered by the parties to be included in an NDA.

Choice of law

There is great uniformity in the law of trade secrets in the U.S. due to the Uniform Trade Secrets Act that has been adopted by 47 states (except Massachusetts, New York and North Carolina), so the law selected to govern an NDA should not usually make much difference in its enforcement.

Choice of forum

If a state is selected for adjudicating claims under an NDA then the party not in that state will be at a major disadvantage if there is litigation. A compromise is not to select a state and each party can then sue the other wherever there is jurisdiction over the party.

How do you mark documents as confidential?

Most often, trade secrets are communicated in a tangible form, whether in hard copy or digitally. It is important that all of these documents be marked in such a way so as to indicate that you consider them to contain confidential information. As discussed previously, you must make reasonable efforts to maintain the confidentiality of your trade secret information, otherwise such information will no longer be considered trade secrets (which means that even with an NDA, a recipient of that information may freely disclose and use such information). Marking documents as confidential is important for demonstrating efforts to maintain the trade secret status of the information in the documents.

A document may be marked as confidential at the beginning of a document, and/or in headers and footers. You can simply insert the word "Confidential," or "ABC, Inc. Confidential Information."

The most conspicuous way to mark a document is by placing a legend at the beginning such as the following samples:

General:	"THIS DOCUMENT CONTAINS CONFIDENTIAL INFORMATION OWNED BY [COMPANY NAME]. UNAUTHORIZED DISCLOSURE IS PROHIBITED."
For submitting a proposal:	"THE CONTENTS OF THIS PROPOSAL CONSIST OF TRADE SECRETS THAT ARE THE PROPERTY OF [COMPANY NAME]. THE CONTENTS MAY NOT BE USED OR DISCLOSED WITHOUT WRITTEN PERMISSION FROM [COMPANY NAME]."
For potential investor/purchaser:	"THE INFORMATION CONTAINED IN THIS [NAME OF DOCUMENT] OF [COMPANY NAME] IS CONFIDENTIAL AND PROPRIETARY. WE ARE SUBMITTING THE INFORMATION TO YOU SOLELY FOR YOUR CONFIDENTIAL USE. UNLESS YOU OBTAIN OUR PRIOR WRITTEN PERMISSION, YOU MAY NOT RELEASE THESE MATERIALS OR MAKE

ANY COPIES, OR DISCUSS THE INFORMATION WITH ANY PERSON OTHER THAN YOUR LEGAL AND FINANCIAL ADVISORS. IN ADDITION, YOU MAY NOT COPY OR USE IT FOR ANY PURPOSE OTHER THAN EVALUATION OF THE COMPANY."

For email communications: "THIS EMAIL MESSAGE AND ANY ATTACHMENTS ARE CONFIDENTIAL AND PROPRIETARY INFORMATION OF [COMPANY NAME]. IF YOU ARE NOT THE INTENDED RECIPIENT, PLEASE IMMEDIATELY REPLY TO THE SENDER OR CALL [NUMBER] AND DELETE THE MESSAGE FROM YOUR EMAIL."

Where should the legends be placed? Legends should be conspicuous and appear on all documentation, whether in hard copy or digital form, such as source code files, databases, notebooks, product plans, roadmaps, specifications, and customer lists. You should err on the side of over marking rather than under marketing documentation with legends. The legends and markings can be done electronically or with a manual stamp.

Note that mere marking a document will not usually bind the recipient of the document without further measures, like an NDA, because just by accepting a marked document, there is no express acceptance of confidentiality restrictions. An example of this would be the mere submission of a response to a proposal. By just marking the response as "confidential" does not necessarily bind the recipient.

What are the risks when receiving confidential information?

By entering into an NDA and receiving trade secret information, the receiving party assumes responsibility and can face serious consequences for breaches. The consequences of a breach of confidentiality can include an injunction and potentially high damages. Therefore, entering into an NDA should not be taken lightly. Liability will not only arise from intentional disclosure, but also from negligent disclosure – and, depending upon how the terms of an NDA are drafted, even by a non-negligent disclosure (i.e., liability without fault).

How do you manage confidentiality obligations with employees?

Employees both access and create confidential information. All employees should sign an NDA. In addition, procedures should be implemented such as (1) orientation session with each employee when first hired, (2) preparation and distribution of an employee handbook that includes handling and responsibilities for trade secrets, (3) annual notices to employees

confirming trade secret procedures, and (4) exit interviews with all employees upon departure where obligations are reviewed with the employee and confirmed in writing.

All of the above procedures put an employee on notice that the employee will have access to confidential information and that the company takes the protection of that confidential information very seriously. If the company is lax in its procedures, an employee might take that as a signal that the company will not take action if there is a disclosure. Whereas, if a company is vigilant in its procedures, the opposite will be the case.

Upon a resignation or dismissal of an employee, the exit process should be quick, all network access and passwords should be secured, obtain return of all devices and documents in the employee's possession, and conduct an exit interview and obtain a signed acknowledgement from the employee.

What is a trade secret inventory?

It is prudent for a business to regularly take an inventory of its trade secrets and validate whether the trade secrets are being reasonably and properly protected. The following questions should be asked and answered as part of such an inventory: What are our trade secrets? How important are they? Where are they located? Who has access to them? Are all people with access subject to confidentiality restrictions?

You may be just starting out and have only a single trade secret. However, if you have been in business for multiple years, chances are that you have accumulated many trade secrets. Also, maintaining an inventory of trade secrets and documenting procedures in place to protect the trade secrets will increase the likelihood that a court will agree that the information actually qualifies as a trade secret.

How to handle non-competition, non-solicitation, and inventions ownership?

Non-competition, non-solicitation and inventions ownership provisions are important ways to protect business information, but are rarely found in an NDA. These provisions will more likely be found in employment agreements, consulting agreements, partner agreements, distribution agreements, development agreements, etc.

What is the Defend Trade Secrets Act?

The Defend Trade Secrets Act became effective May 11, 2016. The act provides a federal cause of action: "An owner of a trade secret that is misappropriated may bring a civil action under this subsection if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." 18 U.S.C. § 1836(b)(1). Possibly the single most important

provision of the act is the availability of ex parte seizure orders. These are available not only as a remedy but also to preserve evidence. The act also specifically protects information provided in confidence to a government official or to an attorney solely for the purpose of reporting or investigating a suspected violation of law. Following from this protection, the act requires employers to notify employees of these protections. Failing to comply with these requirements may preclude the employer from securing either exemplary damages or attorney's fees against an employee who was not provided the required notice.

The remedies available under the act are strong, including (1) recovery of actual loss, (2) recovery of unjust enrichment caused by the misappropriation that is not adequately compensated by its actual loss, and (3) recovery of a reasonable royalty for the unauthorized disclosure or use of the trade secret.

What if someone violates the NDA?

If someone violates your NDA or you anticipate that someone might violate your NDA, you need to act quickly. Delay can be dangerous, as you can lose all trade secret protection. The first steps are to verify that other information has been secured, especially in the situation of a network being hacked, and to consult with legal counsel.

To enforce a trade secret, a plaintiff must bring proof that the information is (1) generally unavailable, (2) has value, and (3) has been protected. Upon a breach, begin to assemble evidence to satisfy these requirements.

Can you license a trade secret?

Trade secrets are a form of intellectual property and can be licensed. A license for trade secrets is very different than for software, but under certain circumstances can be a useful way to monetize the trade secrets.