What Every Manufacturer and Distributor Needs to Know About
Protecting Your Trade Secrets and Internal Proprietary Information

Believe it or not, in today's business setting, your internal proprietary information, including your "trade secrets", is the biggest asset your company has and, as you are reading this sentence, there are plenty of people and organizations out there waiting to get their hands on it. Your competitors would love nothing more than to snatch your manufacturing techniques and implement them on a new product line. Your employees are downloading your customer lists as they plot their next venture and launch party (don't bother waiting for the Evite, you are not invited). These information thieves are numerous and they will stop at nothing to disgorge you and your company from the methods, procedures and formulas that you have attained through years of hard work and at great expense. So you are probably asking yourself, what can be done to protect me and my company against these information bandits? The short answer: EVERYTHING. This article is meant to be a general guide for you and your organization to follow to take relatively easy and cost effective steps to drastically decrease the odds of your business' information falling into the wrong hands.

What Internal Proprietary Information Should You Protect?

The fact that you are looking for information about protecting your business' internal proprietary information is a great first step. The next question you should ask yourself is, how do I know what is protectable and what is not? The following is a non-exhaustive list of the biggest information threats my manufacturing and distribution clients face:

(i) Trade Secrets: protectable trade secrets are generally defined as any formula, pattern, device or compilation of information which is used in one's business, and which gives the business an opportunity to obtain an advantage over competitors who do not know or use it. Courts throughout the United States and abroad have carved out specific instances as to what, and what does not, constitute a protectable trade secret and these specific instances are beyond the scope of this article. Unfortunately, in many cases, the question of what is protectable and what is not is often decided by a judge or jury after years of litigation and at great expense. If you are in a position where you are not sure if you are dealing with a protectable trade secret, some factors the courts will consider are: (a) whether the information is known to others (within or outside of your business); (b) if and to what extent you are trying to protect the information; and (c) the expense you have incurred in obtaining the information. Keep in mind, that general knowledge or mere knowledge of the intricacies of a business is not enough to rise to the level of a protectable trade secret.

(ii) Customer Lists and Supplier Lists: in most cases, customer lists do not rise to the level of a protectable trade secret. It is critical to protect your customer lists and ensure that your competitors do not get a hold of this information. Similarly, information concerning your relationship with your suppliers should be considered extremely sensitive as it could be your competitive advantage over your competitors.

(iii) Pricing/Marketing Data or Strategies: generally speaking, pricing and marketing strategies will not be a protectable trade secret. Even if not considered a "trade secret", the importance of maintaining this information under your roof probably doesn't need to be explained. Should your competitors obtain this information, you can imagine how difficult it would be to compete with them.

(iv) Other Internal Data: when you finally set out and establish your internal compliance procedure, you must make every effort to keep *all* of your business information within your organization, including information you may not currently believe to be confidential. For example, you must treat, as confidential, any information concerning: (a) unannounced product(s) or services; (b) employee compensation or benefits information; (c) sales information; (d) methods of loss prevention, (e) customer complaints customer correspondence; (f) equipment information; (g) material or recipe information; (h) office manuals; (i) software or hardware used, etc.

For the purposes of this article, this information will collectively be referred to as "Internal Proprietary Information".

Complete Protection of Your Intellectual Property is Possible

Knowing what internal proprietary information utilized in your business is protectable alone is a good start but this information by its self, without decisive action on your part, is useless. In order to be fully protected against the information thieves of the world, you must take a proactive approach to deter others from (a) obtaining your Internal Proprietary Information; and (b) in the event someone does obtain you Internal Proprietary Information, preventing that person or organization from disclosing or using the information to their advantage (and your disadvantage).

Proactively Protecting Your Internal Proprietary Information

The following procedures should be immediately implemented into your business to avoid disclosure of your Internal Proprietary Information.

(i) Steps to Take to Avoid Others from Accessing your Internal Proprietary Information - all too often, I see organizations giving third parties

and/or employees complete access to an organizations' information, whether intentionally or unintentionally, without blinking an eye. My rule of thumb is that if you would not trust the person with your ATM card and pin, do not trust them with all of your organizations' information. The information you are giving them unfettered access to is probably worth much more than the money in your checking account. However, many people believe that allowing the access is an unavoidable business risk, and do not perceive the value of the information within the organization. It is critical to change your thought process about the value of the information within your organization and to acknowledge that implanting simple procedures will drastically decrease the odds of the unauthorized dissemination of your Internal Proprietary Information.

(a) Do Not Disclose: The best way to deter these third parties from disclosing your Internal Proprietary Information to your competitors is to not allow access to it in the first place. For example, instead of giving an outside marketing firm complete unregulated access to all of your customer information, you can give a small sample of your customers, or better yet, give a description of your customers purchasing habits, trends, etc. To the extent possible, you should never provide information to third parties unless it is *absolutely* required. Even if you trust the person you deal directly with, you can assume that any information you provide to that person will be easily accessed by others in that persons' company. This information will eventually wind up on the servers of the third party's organization and thousands of other individuals could probably access this information if and when desired. Why tempt fate?

(b) Technology and Password Protection: There are many situations where your Internal Proprietary Information will be stored on computers or servers in your organization. When possible, this information should be stored only on computers that are not accessible to every employee within your organization. If the computer systems within your organization are not equipped to limit the access to others, it is a very important to update your hardware or software to make this possible. All information that you believe is important to keep under your roof should be password protected and only accessible to those who "need to know".

(c) Don't Write It Down: Someone once told me that I should never write anything down unless I would be comfortable with it being posted on the cover of the New York Times. When possible, keep important information in your head and do not write it down at all. Obviously, some information is too great to remember but most of my clients have information

that they keep to themselves in case an infiltration occurs.

(d) Marked "Confidential" Hard Copies Only: I have some clients who refuse to keep highly sensitive material on servers at all. After the document is drafted, they print it out, mark it "Confidential", purge it from their computer systems and keep limited copies in their personal safe. This method is probably considered "old school" and may not work for your organization, but, if possible, it is a great method to keep others from accessing the information.

(e) Properly Destroy Information: If you are no longer utilizing the information or you have updated the information so that other documents are obsolete you must properly destroy those documents so that they cannot be utilized in any way. This also includes permanently deleting all electronically saved documents and e-mails in your computer system, as well as, properly shredding all paper information. Additionally, there may be information stored in other, less traditional, locations such as copy machines, scanners, printers, old computers, etc., which must be properly disposed of.

(ii) Steps to Take When Non-Disclosure is Unavoidable – in many cases, not disclosing or giving others access to information would actually hurt your business due to the fact that things would not get done. When disclosing your Internal Proprietary Information is unavoidable, the following steps are critical to limiting the exposure of the information disclosed.

(a) Properly Drafted Non-Disclosure Agreements: In many instances, disclosing your internal proprietary information to third parties will be required to accomplish the task at hand. For example, if you are undertaking a direct mail marketing campaign, you will probably have to provide the names and addresses of your customers to the organization preparing the labels. When disclosing this information is necessary, you must have a properly drafted Non-Disclosure Agreement ("NDA") signed by the third party organization *prior* to you sending this information. Many NDA's that I have come across are not even close to being suitable to protect the information being disclosed. It is critical that you have a qualified attorney review your NDA before handing over your information or beginning discussions/negotiations. Also, you must require that those receiving the information sign the NDA, no matter what the circumstance. Many organizations think that NDA's are only required in situations where they are actively involved in potential transactions with a competitor or potential competitor. This should NOT be your organization's policy. With the *possible* exception of your attorney, who

Five Keys to Effective and Enforceable NDA's

1. Make sure that the information you are seeking to protect is "protectable" and avoid being overly broad by specifying the information that should not be disclosed as best as possible;
2. Make sure the signor has the capacity to bind the restricted organization;
3. Make sure there is a clause stating that injunctive relief is a possible remedy in case of breach;
4. Make sure NDA is binding in State/Country referenced in NDA; and
5. Make sure ALL individual recipients of the information sign the NDA.

is bound by other means not to disclose your information, every disclosure of Internal Proprietary Information should be preempted with a properly drafted, fully executed NDA, including your marketing company, your accountant, your IT company, your shipping company, your importer/exporter, etc.

(b) Properly Drafted Non-Disclosure Clauses in Business Agreements: Although related to the paragraph above, I want to make an important point that the use of non-disclosure covenants are not restricted to NDA's alone. It is critical to import non-disclosure language in every business related contract involving your Internal Proprietary Information. For example, if you are purchasing or selling a business, your asset purchase or stock transfer agreement must contain a clause stating that any information exchanged will be kept confidential. Similarly, your internal corporate governance documents should require all those with an equity interest to refrain from disclosing your organization's Internal Proprietary Information without consent of the other equity owners.

(c) Non-Competition Agreements: Courts generally disfavor Non-Competition Agreements due to the fact that they may stop a person from making a living and ultimately becoming a public charge. There are instances, however, where a Non-Competes may be an effective deterrent for those looking to utilize your Internal Proprietary Information for their own personal gain. Many court cases concerning the unauthorized use of an organization's Internal Proprietary Information result from an employee [now former employee] downloading all of a businesses' information the day of his or her departure from the company. In certain instances, you may be able to stop the employee from taking a position in a competing organization or preventing the person from utilizing certain information he or she obtains for his or her benefit or the benefit of your competitor. In my opinion, even if not enforceable, the non-compete language has value, in that, it may put some doubt in that employees head which would decrease the odds of the information being taken or disclosed.

(d) Utilize Technology to Fullest Extent Possible: In many cases technological advances are the reason why your information is at risk and accessible to others. At the same time, technology could be your savior against

those seeking your information. For example, there are many software and hardware alternatives that would allow you to trace where the information originated from. Not only does this act as a major deterrent for those thinking about disclosing the information, it would enable you to ultimately kill the problem from its root. Limiting technology to people within your organization can also be valuable. As an example, when the threat is within your organization, those who have access to your Internal Proprietary Information should not have the ability to store, print, copy or send the information by limiting their access to printers, drives, the internet, etc.

(e) When in Court, Seek Protective Order: Unfortunately, in some cases, issues concerning your Internal Proprietary Information are the subject of litigation and your information must be disclosed to the other parties involved. If you are stuck in this unfortunate situation, you must advise your attorney that you consider the information being disclosed important and confidential and you must be sure that your attorney seeks a protective order so that this information will not be disclosed by the other parties. For the most part, documents involved in civil litigation are a matter of public record, meaning, that anyone could have access to them. It is important to seek some type of protection from the court for these documents at the earliest possible stage of the matter.

(f) Settlement Agreements: Similar to a protective order, once a dispute arises and the parties come to a final resolution (whether it is before or after litigation), your settlement agreement should provide for an ongoing obligation between the parties not to divulge any information concerning the dispute.

Implementing Procedures to Protect Your Internal Proprietary Information

Many of my manufacturing and distributor clients do not understand the importance of properly maintaining their Internal Proprietary Information until they get a call from one of their customers stating that their former employee called them to solicit business directly from them. I rarely get a call from a client stating that they want to preempt disclosure of their important information, rather, I get a call stating that they need to know how they can clean up the mess already created by their failure to adequately protect their Internal Proprietary Information [which, incidentally, will be the focus of my next article on this topic]. The goal of this article is to provide you with some of the initial internal steps you can take to prevent the unauthorized disclosure of your business information and taking steps to reduce the odds of the improper disclosure and, ultimately, needless litigation and loss of business. You must understand one thing, reading this article alone will not protect your

business in any way. You must dedicate yourself to implementing these policies in your everyday business procedures. Immediately after reading this article, it is critical that you do the following:

- Speak to your business partners and top level management about the proposed changes.
- Review your employee and procedural handbooks to ensure compliance with the new procedures and make changes where necessary.
- Speak with your IT personnel regarding the upgrade of your hardware and software to implement your new procedures.
- Properly destroy all unneeded information.
- Speak to or hire a qualified attorney to review all contracts/legal documents pertaining to your Internal Proprietary Information and make sure the provisions would be enforceable.

About the Author

Brian A. Lincer is an experienced business and intellectual property attorney who represents organizations that manufacture, import, sell and distribute products within the United States and abroad. Mr. Lincer focuses his practice in matters concerning licensing, intellectual property, product labeling and regulatory compliance, including issues relating to trademarks, copyrights, patents, trade secrets, Federal Trade Commission [FTC], Consumer Product Safety Commission [CPSC] and California's Proposition 65. Mr. Lincer is the publisher of the "Footwear and Apparel Protection Law Monitor" and a regular contributor to businessandfranchiselaw.com. Mr. Lincer also provides outside general counsel services for numerous organizations with regard to various business, licensing and intellectual property matters. Whether you have questions about filing, maintaining or enforcing your intellectual property, questions about establishing a compliance program within your organization or have questions concerning a specific commercial agreement, **click here** to contact Mr. Lincer to discuss what specific options are available to you.

Call: 1.800.976.4904

Email: blincer@dddilaw.com

Web: www.businessandfranchiselaw.com