RICHARD ARMSTRONG ESQ

8 LEGAL TIPS *for* SMALL BUSINESSES

INTRODUCTION

If representing business owners for forty years has taught me anything, it is this simple fact: there is no more courageous group of men and women on the planet. Whether barely out of school and starting from scratch, or a retiree looking for new worlds to conquer, the entrepreneur who ventures forth to do war in the marketplace is at once valiant, and indispensable to the American way of life that is the envy of the world.

I have asked myself many times why, as an attorney in private practice, I chose to set up a law practice geared to representing such folks. Here is what I keep coming up with. Because I didn't decide to go into business myself, I receive a vicarious thrill from representing those who did. In some sense, I get to share in their victories and failures, their longings and disappointments.

I get to do battle for them, negotiate for them, help them with aspects of planning their business or businesses, and counsel them on how to safeguard their dreams. I get to step into their shoes, if only for a moment. And in some sense, I am a kindred spirit because, after all, I did set up my own law practice years ago.

Over those years of representing businesses, some big, some small, across many different industries, I have learned that there are certain commonalities that bubble to the surface and resonate with every business owner, whether there are hundreds of employees or only a few. Please understand that I am defining small business as five hundred employees or less. Admittedly, the definition is somewhat arbitrary, but the dynamics applicable to small businesses hold true for nearly every business falling within this bracket. Because the dynamics are consistent, so are the legal issues that arise with these businesses.

And so, I have elected to address certain commonly confronted issues, together with "tips" on how to avoid these problems altogether, or at least reduce their negative impact on your business. In doing so, I've endeavored to reduce these pearls of wisdom to the most condensed, readable format possible—a herculean challenge for a man who makes his living with words! But if anything rings true with the business owner/operator, it is that, "Time is Money". And the more time our clients can save by learning from *someone else's* mistakes, rather than their own, the better their bottom line.

Yes, the law can at times be complex. But most of the time, if a person implements safe practices *preventatively*, he or she can simplify the practical application of legal principles to their business. By doing so, they can significantly lower their chances of winding up in court, in bankruptcy, or of simply being vulnerable to those that would take advantage of them.

It is in that spirit of prevention that I offer for your consideration eight tips I give to our small business clients. They have stood the test of time, and I trust that they will be beneficial to you as you valiantly strive for success in your business.

Richard Armstrong Esq.

TABLE OF CONTENTS

1- Forming Your Business 5

2 - Making Your Contracts Legal 8

3 - Labor & Employment Law 11

4 - Non-Compete Agreements 14

5 - Collecting Receivables 19

6 - Document Preparation & Review 22

7 - Protecting Intellectual Property 25

8 - Data Breaches & Legal Liability 27

CHAPTER ONE

Forming Your Business

It sounds almost trite, to start out a book with the admonition to set your company up correctly. "Of course," you're probably thinking to yourself. "That's a given, and I get it. So now, let's move on to the real stuff so I can get to work." However, I have been representing businesses long enough to know when I see a major area of vulnerability. And, believe me, this is one.

What do I mean? Now I'm going to pick on a favorite talking point. In the last 10 to 15 years, we've witnessed a paradigm shift in the legal world. It has affected nearly every area of the law, but few as much the law governing businesses. Why? Simply stated, the reason is convenience.

With the advent and ubiquity of the Internet, forming a new company—at least in the most rudimentary sense—has become as easy as filling out an online form, inputting a credit card number, and clicking "Enter." I can't tell you the number of new clients visiting my office annually that bring me their company records, spread them out on my desk, and begin discussing their structure with the confidence of a C Suite executive.

More than half of those clients have given no thought whatsoever to the type of entity that would best serve their needs in the industry in which they operate. In fact, some are involved in a dispute that may well lead to a lawsuit. Others are already in the middle of a lawsuit. By that time, it is too late to change the type of entity they selected if they made a poor decision. As merely one example, limited liability companies are appropriate for some businesses, where an S corporation or C corporation would be a better choice for a business in a different industry.

Factors such as whether you plan to sell your business down the road, seek investors, or "go public" should influence your choice of entity. Just one example: if you are going into the oil and gas business, you will need to consider a much different structure than if you are opening a retail store or an insurance agency.

This situation is further complicated by the increasing proliferation of certain services—whose advertised names you will doubtless be familiar with—that purport to provide all the forms necessary for you to properly set up your company in a particular state, at a cost reputed to be less than hiring an attorney.

While there is nothing wrong with trying to save money, each one of us can think of situations where we tried to save money initially, only to learn that, in the final analysis, we spent far more than we would have if we had hired a professional to do the work. In my experience, this occurs most often in the professions and in highly technical fields.

What if someone told you that you could diagnose and treat an illness much more cheaply by reading a certain self-help book that cost $14.99, rather than incurring the significantly higher cost of visiting a physician? Although this might be attractive for a simple cold, I suspect you would be reluctant to forego medical treatment for a more serious illness. Or, suppose that you had a tooth that was cracked and causing you pain, and a friend recommended a good pair of pliers and a brochure telling you how to remove it for a fraction of the cost of a dentist or endodontist? You can see where these hypotheticals are going: What may seem simple on the surface can prove to have negative and long-lasting repercussions when you have no training or don't know the possible consequences.

While there may not be as much to lose when a sole proprietor decides to set up a company and is the only stakeholder, your downside risk increases significantly when additional owners become involved. Where there are multiple owners, the human potential for disputes and quarrels rears its ugly head. At that point, if no proper written agreements are in place to deal with the contingencies, the only remaining path may be directly to the courthouse: a situation no one wants.

If one of the owners wants to leave the company, dies, or gets divorced, a myriad of complications can and do occur. There needs to be a legal path that allows an orderly way to resolve these very common, yet potentially divisive, issues. The bottom line is that it is far wiser, and ultimately far less expensive, to have a seasoned professional advise you on the best type of entity for your needs and to set it up, than for you to do it yourself with an online form. The initial setup of your company can also evolve into a trusted, long term advisory relationship in which your attorney will develop and review the required vendor agreements, industry regulations, employment contracts, and other policies for your company.

Conclusion: Set up your company correctly from the outset to avoid potentially divisive issues later on.

CHAPTER TWO
Are Your Contracts Legal and Enforceable?

"Get it in writing." Have you ever heard that time-worn maxim? It rings true now more than ever, with the plethora of emails, texts, and videos flying around through digital space. Business owners and operators are mindful of the importance of this maxim, but they don't follow it—at least, not consistently. And then, when a lawsuit is filed, those owners are caught, so the saying goes, with their pants down.

Many first-time business clients think they've got themselves covered because they have a legal form that they procured from someone in the same line of work, or even a past employer. Scrutiny of those documents, however, usually reveals a semi-legible copy of a copy, with outdated terms.

By "outdated" I mean that the contract, even if otherwise acceptable, has outdated references to the law, or doesn't even reflect drastic changes in the law that have occurred since it was first drafted. Just because someone they knew or formerly worked for is using the document doesn't make it reliable. In fact, the misplaced confidence of a business in such outmoded contracts is a very dangerous thing.

We have also seen contracts in this office that were not really contracts at all, because they have missing pages, missing terms, or lack of legal consideration, or quid quo pro. This is made worse still by the fact that we live in a rapidly changing world which promotes an "anything will do" kind of communication style.

Whenever an email can be used where a written document was formerly needed, a party fires one out. If the email is responded to affirmatively, the participants believe they have a contract. Increasingly, the same phenomenon is occurring with text messages. And while a recorded audio or video conversation is better than nothing at all, it is far inferior to a properly drafted and signed document. Why? Because emails, texts and recorded conversations invariably leave out critical components of a contract.

At the end of the day, it remains for the parties' attorneys to cobble together fragments of these informal agreements into a unified, meaningful whole—a task which can be near to impossible after they are already in use. This is precisely what keeps business litigators in business. Incompleteness creates ambiguity, and ambiguity invites litigation. Litigation, the bane of every company, is a double curse. Not only can it cost you a significant amount of money, but it also robs you of your most valuable asset: time. And time away from your business is money lost.

Properly drafted and executed agreements perform yet another vital function. They memorialize the agreement. That way, when the business is sold or a son or daughter takes it over from you, there is a definite reference point as to what was agreed to, when, and for how long. There is something inherent in a signed instrument, even if it is E-signed, that makes the courts regard it with a degree of respect.

That is one of the reasons that, when we are preparing formal documents for our business clients, we go through several drafts to get it right. Sometimes we do so because our client and the other attorney's client are negotiating. More often, we just want to make sure everything has been thought out and covered, and nothing is left to chance. By doing this, we make our

clients think about things that never occurred to them, in the interest of heading it off before it later becomes a problem.

Finally, "deterrent value" plays an important role for partnership agreements, corporate documents, or contracts with third party vendors or investors. This concept operates much the same way as the relationship of the Unites States with other superpowers that maintain an arsenal of missiles, drones, and sophisticated weaponry in the hope that they will never have to deploy them. Knowing that the United States is "armed and ready" serves as a deterrent for any country who might otherwise act recklessly with us.

Similarly, when business partners, customers, or would-be antagonists see that you have well-crafted legal documents, it deters them from risky behavior which would be detrimental to your interests. They reason, usually correctly, that anyone who took the time and spent the money necessary to have their documents properly prepared by an attorney, would certainly back them with legal firepower if challenged.

This is precisely the respect you want to engender when you deal with others in the business world. Don't misunderstand: it does not mean that terms are never subject to negotiation. But it does mean that you negotiate from strength, not weakness, to achieve the results you expect and deserve.

Conclusion: Have your critical documents prepared by an attorney to ensure that they are legal, enforceable, and a deterrent to reckless conduct.

CHAPTER THREE
Labor & Employment Law

Discontented Employees

The problem of discontented employees is pervasive. The reason? The federal government, and certain states in particular, avail employees of more legal rights than in many foreign countries. These rights range from those conferred by union collective bargaining agreements to whistle-blower statutes, the FLSA and similar laws governing overtime and minimum wages, OSHA, the Americans with Disabilities Act, Age Discrimination in Employment Act, and working conditions in general. Trying to interpret all the above without expert legal counsel can present a slippery slope for unwary business owners.

The first step in protecting yourself from litigation is to set up a standard process for both hiring and firing. Ideally, this should entail documentation relative to the different types of positions in your business, as well as an employer policy manual, and documents tailored to termination or separation.

If the procedures are uniformly adhered to, it will go far toward protecting you from frivolous lawsuits, claims filed with the state labor board or commission, and even work-related injury claims. If you are a large enough employer to trigger a majority of the above-mentioned statutes, the manual you finalize should address each one, at least in summary form.

Claims of Discrimination or Harassment

Nothing can bring a company to its knees faster than a federal investigation into claims of workplace discrimination, sexual harassment and the like. To help prevent this from happening, it is best to follow a planned approach in interviewing that has been approved by legal counsel.

Although systemic discrimination is less likely to occur in small companies than large ones, businesses that range in size from 50 to 135 employees are definitely big enough for cliques to form and discriminatory conduct to take root. It is therefore advisable to keep on hand all resumes received, as evidence that you hire qualified people from a diversity of candidates regardless of their age, race, ethnicity or gender.

It's also important to have your legal counsel hold meetings with your managers to school them on how to discourage harassment and eliminate offenders before they become a problem. By adopting and enforcing regular policies, and holding meetings where necessary, you will weed out these problems before they begin to grow. Then, yearly maintenance will keep them out.

Illegal Immigrant Employees

Documented processes and procedures should be in place to readily identify employees that don't have the right to legally work in the United States. Regular checks of your workers, including random background checks, can help prevent you from employing individuals who are in the country illegally. It is not uncommon for certain businesses to falsify immigration documents. If the federal government uncovers this deception during an immigration audit, it can in some cases shut down a company, sometimes permanently.

Intellectual Property Issues

If your firm routinely creates proprietary, novel or creative products, such as in the high tech or entertainment fields, aggressive patent, trademark, or copyright litigation can be a pervasive threat. As merely one example, some enterprises now deliberately acquire and hold onto patents for years, banking on the prospect of one or more companies unknowingly violating them. They then make a

business out of bringing lawsuits to collect on patent violations. The good news is that it is not hard to avoid this risk.

When working on product development, have your R&D team routinely research the patents, trademarks and copyrights applying to each product. Doing so will head off an otherwise bloody and expensive legal contest in the event you allegedly wander into someone else's IP "territory".

Conclusion: Have your legal counsel set up protective measures to minimize risks from (a) discontented employees, (b) discrimination or harassment claims, (c) illegal immigrants posing as documented workers or citizens, and (d) claims of intellectual property theft or misappropriation.

CHAPTER FOUR
Employee Non-Compete Agreements

Let's say you have just learned that a former key employee of yours may be violating the terms of her non-compete agreement with your company. What should you do? Should you call her and ask that she stop? Should you ask your attorney to send a letter threatening her with prompt legal action? Or should you immediately file for a temporary restraining order or injunction without notice? While you may ultimately execute *all* of these actions, your initial step should be to gather the evidence that will support your claim of violation, and you should move as quickly as possible to accomplish this.

Before you alert the employee that you are aware of her activities and spend many thousands of dollars in attorney's fees pursuing a temporary injunction—we suggest an ordered approach to help you evaluate the strength of your claim against this individual. This step-by-step method will also help you gather the ammunition that you will need if you *do* decide to proceed.

First Step: Identify and Gather Relevant Evidence

You need to learn as much as you can about the employee in question and any agreements that she might have signed with your company that might contain a post-employment restriction on her activities. Look for the following documents in the employee's file:

(1) offer letters;

(2) employment applications;

(3) employment contracts;

(4) non-competition agreements;

(5) stock option agreements;

(6) non-solicitation agreements;

(7) separation documents the employee might have executed as part of such agreements;

(8) settlement agreements containing any releases of claims;

(9) if there was a merger and acquisition, documents that she may have executed as part of that transaction;

(10) any other agreements she signed that contain any post-employment restrictions.

As you peruse your records for the above items, bear in mind that older non-compete agreements can take the form of a "stand-alone" document. But more often, the non-compete will be an integral part of one or more of the above documents.

Second Step: Assess the Strength of the Evidence

Now that you have gathered all the documentary evidence, did you find an employment contract which contains a non-compete covenant? If so, your attorney will need to analyze it to determine if it has the requisite hallmarks of an enforceable non-compete agreement under Texas law.

If the contract states that another state's law applies to the employment contract, your attorney will check that state's law to see whether it will be enforceable. One issue will involve his determining whether adequate legal consideration passed between the former employee and your company at the time the contract was signed.

The consideration can sometimes be found in the employment contract itself, but often it comes to light by reviewing some of the other documents on your evidentiary list. For example, if stock options were given to the employee at the time the employment contract was signed, that will probably be sufficient to support the non-compete covenant. Such consideration is strengthened if the employment agreement specifically references the stock option grant and why it was given.

If there was a non-solicitation agreement--different from a non-compete covenant--it will normally appear in an employment agreement, but may also be a separate instrument. Your lawyer will be interested to see this, and to hear about the circumstances of its signing.

Third Step: Analysis of the Documents You Found, and Their Effect on Each Other

What your attorney will do with the material you have provided to him is to thoroughly sift through and analyze each employment agreement, stock option or other employment benefit; stand-alone non-compete covenants; non-solicitation, and trade secret protection agreements (sometimes buried in Non-Disclosure Agreement a/k/a "NDA"); or invention or work-for-hire agreements.

His job will be to synthesize all such agreements to see if, either together or separately, they provide the necessary legal consideration to support reasonable restrictions on the right of an individual to work for any one that he or she chooses. He may well involve you in this process, particularly if the documents present an ambiguous or confusing picture on the sequence of events during your former employee's tenure.

It is not uncommon, in the hurried pace of small business, to discover undated or partially signed documents, agreements with missing or partially legible pages, missing originals, or even documents which have vanished altogether. While these are never the optimal situation from an evidentiary point of view, they need to be confronted well before a decision as to whether to litigate is made or a strategy is laid out. Your involvement with your attorney at this stage will help fill in the gaps in the evidentiary record and resolve any apparent factual conflicts or ambiguities.

Fourth Step: Decide Whether to Make Demand and Sue

Once your attorney has met with you to discuss the strength or weakness of the written and oral evidence, it is time to make an informed decision about whether, and in what form, to take action against the competing party. Although it may seem like a foregone conclusion that you take prompt legal action against a former employee acting in violation of his or her contract, your attorney should advise you to avoid a knee jerk reaction.

Like any other business decision, you should weigh the benefits against the risks and downside costs. Some companies have made it a policy that no matter the cost or the circumstance, they will pursue judicial relief against such an employee. This is an acceptable option for some firms, but one that most can ill-afford.

This type of litigation is "front end loaded," meaning that it costs more than the typical lawsuit for damages by its very nature. A step short of this approach, now that you have your evidentiary ducks in a row, is to at least send the offender a thoughtfully worded demand letter that sets out in broad strokes what you know about the former employee's activities, and what the consequences may be to him if such actions do not cease or are modified to a level you can live with.

We recommend that you decide ahead of time just how far you are willing to go beyond this point, and how much money you are willing to spend, to secure compliance. If you don't have what it takes to see it through, don't go farther than the letter. Cases such as this can quickly take on a life of their own, and once you become invested in the process, it is very hard to extricate yourself from without looking somewhat foolish.

The result, in the event that occurs, could be just the opposite of what you wanted to do: establish a firm, no-nonsense reputation that acts as a deterrent to unfair competition. Above all, let your attorney guide you through the pitfalls, both before and after you make the decision regarding what steps to take. He has been down this road before, which has land mines buried along the way. He can help you do an astute evaluation of the risks and benefits involved in the litigation process.

Conclusion: If a current or former employee is competing with you in violation of an agreement that he/she signed, move slowly and deliberately through the evidence, and make a careful and informed business decision, assessing costs and benefits with assistance of legal counsel.

CHAPTER FIVE
Collecting Receivables

When you're in business, people owe you money. Nearly every business owner has at least a few slow-paying customers or clients—and when they fail to pay, it can hurt the bottom line. For this reason, business owners should follow certain basic protocols and procedures in attempting to collect their accounts receivable, both to protect the customer relationship if it is salvageable, and to stay well within legal bounds.

For best practices, I recommend businesses follow the guidelines of **the Fair Debt Collection Practices Act (FDCPA)** and the **Texas Debt Collection Act.** While these laws apply primarily to third-party collection agencies, and not the original creditors, they still provide good signposts and safeguards for business owners attempting to collect debts so they don't inadvertently venture into harassment territory. Additionally, they provide some basic wisdom for sound collection practices. Let's look at a few A/R collection "don'ts" based on these laws:

Don't call your customers before 8:00 a.m. or after 9:00 p.m.

Don't use profane language or threaten violence.

Don't call their accounts payable department multiple times a day.

Don't threaten past-due customers with any specific action you are not willing, or legally authorized, to take. For example, don't threaten to take a customer to court unless you're genuinely ready to take that step. If the customer doesn't pay and you don't follow through with a lawsuit, you will be creating an image of a business that doesn't follow through and may safely be ignored. Additionally, if the case does proceed to court, the customer could turn it against you and make you look like the bad guy.

Don't threaten to garnish wages or put a lien on the customer's homestead. The State of Texas has some of the broadest debtor protection statutes and constitutional provisions of the fifty states. You can only do some of these things in very narrow, specific situations.

Don't continue to call a customer who disputes the debt. Instead, focus on providing proof that the debt is valid.

Now that I have provided you with tips about what *not* to do, what about things you *should* do to collect your outstanding payables? Please understand that this portion of the chapter is not legal advice. But because a law practice is as much a business as any other service enterprise, I can speak as one business owner to another.

The most practical, time-proven tip I can give is to collect your money promptly. I don't know what kind of business you are in, but I can't suggest strongly enough that, if it is possible to do so, get your money at the time of purchase of the product or service you are selling.

I realize that it is customary in some lines of work to bill on 10-day or 30-day terms, sometimes, even longer. But times are changing, largely due to the nearly universal use of debit and credit cards, and the ease of paying online.

Be willing to extend your customers that convenience. Take their payment at the time of sale if possible. If it is not possible simply because "things aren't done that way," then consider offering a small monetary incentive for prompt payment. The old 2/10, net 30 model worked for years. Pay within ten days for a 2 % discount. This can be less or more at your choosing, but be careful that you take into account the merchant fees deducted from the sale and the effect it has on your profit margin.

If you don't, won't, or can't accept debit or credit card payments at the point of purchase or online, then make your terms of payment very clear at the outset of the transaction -- if possible, in writing as part of a contract.

Finally, have your attorney set you up a collection letter series, and *religiously follow the send-out schedule*. Do not—I repeat—do not, vary from your schedule. Accounts that go past more than 30 days become significantly more uncollectible than those that are promptly contacted. Do not be afraid to have your legal counsel send out the last letter, whether you plan on taking legal action or not. This often gets results.

Conclusion: Stay within the bounds of the debt collection statutes when collecting receivables. Accept payment by debit or credit cards, and if possible, get all your money at the point of purchase. Offer discounts for prompt payment. Have firm payment terms stated in your contract. For delinquent accounts, adhere to a rigid collection letter schedule, and have an attorney draft both a review and final letter in the series. Do not let accounts go past 30 days.

CHAPTER SIX
Document Preparation & Review

As a small business owner, paperwork can sometimes feel like the bane of your existence—but in fact, the right paperwork protects your business legally. Aside from the founding documents filed with the state defining your business as a corporation, limited liability company, limited partnership, joint venture or the like, every small business should have a basic set of documents in place to define relationships with business partners, clients, vendors and employees.

Remarkably, many small companies don't have all (or sometimes any) of these documents. Let's run down a quick list of the most essential documents you should have to keep your business functioning smoothly.

Shareholder/Member Agreement

Any business that has more than one owner, partner or investor needs some form of shareholder agreement that specifies who owns what, who is responsible for what, and how the various owner/partners will work together. Businesses without this documentation are a breeding ground for sticky, time consuming and expensive lawsuits, particularly if they break up, or someone dies or divorces.

Employment Contracts/Independent Contractor Agreements

Whether you hire employees, utilize independent contractors or a combination of these, you need paperwork that clearly outlines the scope of these relationships—including company expectations (*think: employment policy manual---see below*), employee/contractor responsibilities, deliverables, terms of payment, etc.

Vendor Agreements

For any third-party individual or company providing supplies or services to your business, you need a vendor agreement that defines those business relationships, including what is being supplied (with a due date), what you will pay, terms for settling disputes, and so on. Sometimes this is supplied by the vendor, in which case, you should have your attorney review it and mark it up as necessary. If not supplied by the vendor, then furnish one that is favorable to you.

Employment Policy Manual

In addition to an employee contract which you should have with each member of your staff, you should also have an employee manual that details company expectations as well as the general rights and responsibilities of your employees. This manual becomes the standard frame of reference—the "go to" document—to expeditiously resolve disputes and enforce policy.

Reviewed Lease Agreement

If you lease office or work space, you should have a lease agreement with the owner/landlord. These leases, often of the "triple net" variety, can be tricky to navigate and often contain terms that are detrimental to the tenant. That's why it is extremely important to have these documents reviewed by an attorney before signing. If you've already signed a lease agreement, have it reviewed to identify weak areas that may support a renegotiation of terms more favorable to you, either now or in the future.

Building Purchase Document

A title company closing the deal is not enough to protect your interests, especially if you are the *buyer* of the new building. The title company is there to sell title insurance, and usually to close the deal on terms favorable to the seller. Again, it's important to have your attorney look at the purchase agreement and point out any errors or unfavorable terms. You will be amazed at what you find.

Other Documents

Depending on the nature of your small business, you may need additional legal documents above and beyond the basic list described above.

Conclusion: All shareholder or member agreements … employment or independent contractor agreements … vendor agreements … employment policy manuals …. lease agreements and purchase documents … should be prepared and reviewed by counsel to ensure that they are up to date.

CHAPTER SEVEN
Protecting Your Intellectual Property

I touched on this in Chapter #3, but this bears going into in greater detail, primarily because of the age in which we now move and operate. Hi speed computers, the internet, and a myriad of personal and wireless devices have increased the probability that, sooner or later, someone will attempt to pirate, misappropriate, infringe or palm off your intellectual property.

If you're in business, you have intellectual property ("IP") to protect, whether you realize it or not. Even if you're a service company or you don't sell anything proprietary, you have a brand, one or more logos, printed materials and perhaps even business methodologies that others could emulate, or even copy and steal if you don't take steps to guard them. Your IP is a key to your business success and competitive position in the marketplace—so how do you keep it safe?

What Counts as Intellectual Property?

First, a definition: The Legal Information Institute defines intellectual property as "any product of the human intellect that the law protects from unauthorized use by others." In broadest terms, this can include any invention or artistic creation (e.g., music, poetry, art). But from a business perspective, IP also encompasses designs, logos, original software or other intangible property that helps you do business differently than others. Anything that can be copyrighted, trademarked, patented or identified as a trade secret counts as IP that you should protect.

Protecting your Business's IP

Common sense things you should do to protect your IP include:

• Apply for patents, copyrights and trademarks as early as possible. Even if your application is denied, applying educates you in the process, and it may be granted on a subsequent attempt (this has happened with yours truly).

• Educate your employees on exactly what constitutes your company's IP, and how to guard your company secrets which are not protected by patent, trademark or copyright.

• Have explicit policies written that apply to protection of IP, and consistently enforce them.

• Share trade secrets and confidential information with employees only on a "need-to-know basis," and make sure all relevant employees know how to protect proprietary information.

• Have your attorney create well-crafted and up-to-date nondisclosure agreements, and make sure your employees sign them.

• Label all your publicly registered and protect ed intellectual property. If it's copyrighted, include copyright information; if it's trademarked or service marked, include the ™ or ℠ symbol. Put it on every piece of printed matter and every computer screen. Remember, labeling your IP is evidence helping to proving your rights in court if someone uses it in an unauthorized manner, and not labelling can be evidence that hurts you.

• Look seriously at whether international patents are necessary. U.S. patents won't protect your property if you use your IP overseas.

The bullet points listed here are just the basics. Providing adequate protection for your company's IP can be complicated. Given the choice, it is best not to attempt to do it without a competent business attorney or IP counsel. But whatever you do, protect it now, then monitor whether it is compromised, or infringed once it becomes well-known, recognized and intrinsically valuable.

Conclusion: take concrete steps to put in place the above safeguards now. Once you get busy and the money starts rolling in, it is very easy to "fall asleep at the switch" until after valuable IP has been misappropriated or infringed.

CHAPTER EIGHT
Data Breaches and Legal Liability

Small businesses are particularly vulnerable to cyberattacks and the data breaches resulting from them. What constitutes a small business varies greatly from industry to industry, but a good average for our purposes is 500 or fewer employees and $20 million or less in gross revenues per year. A full 99.7 % of American business firms qualify as "small business" according to the Small Business Administration.

For reasons discussed previously in this book, a small business presents an easy target for cyber criminals. What makes small businesses so enticing is the utter failure of the vast majority of those businesses to take even modest measures to protect either their client or customer data.

Why is Data Security Important?

"Why should I be so concerned about protecting my customers' data?" you may ask. From a singularly selfish viewpoint, you should be aware that 60% of all small businesses do not survive a cyberattack and cease operations within six months. Or consider the fact that, if a first-tier customer has its data stolen, corrupted, and published for all to see, or vanish completely, you lose more than a customer. That former customer now becomes a dissatisfied customer ready to spread your misfeasance far and wide, through every channel of communication including social media. You can quickly begin to comprehend why, even if you survive the onslaught, your business will never be the same again.

Data breaches have become a more common phenomenon than many may care to admit. It is no longer something we can sweep under the rug, change the subject, and hope no one else notices. In the event that you aren't motivated to put protections in place out of enlightened self-interest, know this … In all but one major area, that being certain Protected Health Information protected by HIPAA, legal responsibility for a data breach falls squarely and exclusively on the owner, not the holder, of the data. Therefore, if you created the data, used pre-existing private data of a customer or client to create your own, or purchased the data under an agreement, it is solely your responsibility to keep the data safe---even if someone else is holding the data on their system. More on this below.

Special Liability Under HIPAA

If sensitive or regulated data such as protected health information (PHI) under HIPAA is stored in the cloud and a breach occurs, the data owner (e.g., a physician's office) is legally required to disclose the breach and send notifications to potential victims. But even if you did not create the data, you may be under special duties as a *holder* of the data.

For example, a personal injury law firm holding PHI is classified as a "business associate" under HIPAA and therefore subject to its legislative reach just as much as a medical practice. The statute, and Business Associate Agreements executed with respect to it, require the data holder to report the data breach to the data owner and assist in the investigation.

State Requirements if there is a Data Breach

Emulating federal law, many states now require notice of data breaches to customers or clients. For example, Texas, where I practice law, requires a person who conducts business in the state and who owns or licenses computerized data that includes sensitive personal information ("SPI") to *notify any individual whose SPI was, or is reasonably believed to have been acquired by an unauthorized person.*[1] If you fail to comply with this notice statute, it can cost you civil penalties of up to $100 per person per day that you delay, to a maximum of $250,000 per data breach.

In addition, effective January 1, 2020, Texas House Bill 4390[2] amended this law to remove the "as soon as possible" notice requirement. Now, the statute requires notifications of such a data breach to be made "without unreasonable delay and…not later than the 60th day after the date on which the person determines that the breach occurred."

This amendment is important, not only because it clearly defines the meaning of "without unreasonable delay," but also because it starts the clock running from when the *actual data breach* is determined to have occurred. Typically, such a determination is made only after a cyber-incident has been fully investigated by an IT professional, so this amendment buys some time for the accused to ascertain the facts.

[1] Tex. Bus. & Com. Code §521.053(b).
[2] Signed Jun 14, 2019

But there is yet another requirement added by the amendment. The statute now requires that if the data breach affects at least 250 Texas residents, the attorney general must be notified during the 60-day time period. Such notice must include 5 described categories of information set out in the statute.

Of course, the *real cost* of such a breach is not the fines that may hit you if you wait to report, but the loss of customer trust and goodwill when you *do* follow the law and report the incident. No one wants to be caught having to explain to clients why they dropped the ball and exposed their SPI, especially in an era when there are manifold ways to protect it. And no one wants the liability that would necessarily follow. Any meaningful discussion about how to mitigate that liability begins with a careful appraisal of the law pertaining to breaches of computer security.

What About Civil Lawsuit Liability?

Over and above the standards and punitive measures ensconced in state and federal statutes looms the threat that an aggrieved customer or client can sue you for negligently allowing their SPI to be accessed, corrupted, disclosed or otherwise mishandled. Earlier in this chapter, I mentioned that it is the owner, not the holder, of the data that is ultimately liable in the event of a data breach. In a "cloud" environment---which more and more of us are now operating in---under U.S. law and standard contractual terms, the data owner is the party that faces liability in the event of a data breach loss.[3]

As hard as it may be to believe, this is so even if the security failures are caused by the *data holder*, or cloud provider. Why is this? Because the standard vendor agreements which cloud providers require you to sign include terms *excluding consequential damages and limiting direct damages*. And in the majority of cases, the damages caused by a data breach of the data (cloud) holder will be considered consequential damages. For this reason, those damages, *e.g.*, loss of customers, lost profits, damages to reputation, will be barred by standard provisions foreclosing all liability for consequential damages.

[3] The exception to this rule is HIPAA - Protected Health information (PHI), which places responsibility on the holder of the information.

What if the Data is Held on Premises?

If the data breach results from a cyberattack on a traditional data owner's proprietary network or data center, the data owner is potentially liable. But just how much exposure would you have in such a case? Current federal and state laws governing privacy do not impose wholesale civil liability triggered by a cyberattack. Generally speaking, liability may accrue where one or more of the following factors can be shown:

- A company failed to effectuate statutorily required safeguards or reasonable security measures (often called *negligence per se*)
- A company failed to either remedy or mitigate any damage following the breach
- A company failed to give timely notice to harmed individuals as required by a state statute governing data breach notification. This may give rise to *civil penalties* imposed by a state attorney general or other regulatory agency, but may also be used to establish the *standard of care* in a private civil action for negligence.

Irrespective of the presence of the above factors, civil liability for negligence must always be proven by a preponderance of the evidence. Additionally, liability for damages may also be proven on the basis of a contract containing indemnity provisions, or master service or similar agreements between businesses.

The State of Texas Law on Breach of Computer Security

There is a wealth of information available about what one can do at a technical level to protect oneself from cyberattacks and cybercrime. We will not rehash this information here. This chapter, therefore, will not focus on technical preventative measures as much as it will the things you can do legally to protect yourself before a cyber incident occurs. The state of the law in Texas on breaches of computer security has significantly matured in recent years. It is now a crime for a person to knowingly access a computer, computer network, or computer system without the effective consent of the owner.[4]

[4] *See* Tex. Penal Code §33.02, *et.seq.*

Develop a Terms of Use Agreement

Deploying a carefully drafted Terms of Use ("TU") Agreement on your website(s) can be a very effective tool to deter would-be hackers. But such an agreement can also provide victims of malevolent activity an avenue for recovery of damages.

Recently, a Federal trial court held that Plaintiff Southwest Airlines stated a plausible claim for violations of the federal COMPUTER FRAUD AND ABUSE ACT[5] and the TEXAS HARMFUL ACCESS BY COMPUTER ACT[6] in its complaint initiating a federal lawsuit[7] for damages against a company that was allegedly using page-scraping and other automated tools to access or monitor Southwest's website. Southwest's TU Agreement specifically prohibited use of page-scraping and such other automated tools. Because the federal and state statute referenced above prohibits accessing a computer without authorization, and Southwest's TU Agreement *expressly prohibited* such practices, Southwest could maintain its action for damages against Roundpipe - the named defendant in the aforementioned litigation.

Conclusion: Beyond the scope of this article are the technical steps a business owner can take to deter, remedy, or mitigate the effects of a devastating data breach. However, the time-tried maxim, "The best defense is a good offense," holds true here just as it does in football. It is definitely worth the time and money spent to implement a system that is as near hacker-proof as technology and your budget allow. Further, a loss mitigation plan should be in place that will give you at least a chance to restore some normalcy to your business operations. Finally, make certain that your data is fully backed up with a reliable system at all times.

[5] 18 U.S.C. §1030
[6] Tex. Civ. Prac. & Rem. Code §143.001, *et. seq.*
[7] *S.W. Airlines Co. v. Roundpipe, LLC*, 375 F. Supp. 3d 687, 706 (N.D. Tex. 2019)