AN ILLINOIS LAW FIRM

# GETTING DOWN TO BUSINESS

## HEYL ROYSTER
## BUSINESS & COMMERCIAL LITIGATION NEWSLETTER

 **Summer 2013**

## WELCOME LETTER

Dear Friends,

Welcome to our latest issue of "Getting Down to Business," Heyl Royster's newsletter addressing the concerns of small business. As always, we share our thoughts on current issues facing commercial owners and managers from the perspective of our litigation attorneys who represent business entities ranging in size from sole proprietorships to multinational corporations.

In this edition, we focus on the protection of proprietary information. Stacy Crabtree discusses the importance of safeguarding confidential information shared with third parties. Often the sharing of such data is a necessary component of business, particularly with sub-contractors or vendors; however, many companies fail to institute reasonable controls on the uses of this valuable information. Stacy provides insight into controlling the permitted uses of your confidential materials.

Mark McClenathan addresses the protection of confidential information and other legitimate business interests in the context of the employer-employee relationship. Mark shares recent trends in the law demonstrating the complexity of preparing effective restrictive covenants in employment contracts to guard against theft of trade secrets and unfair competition from former employees.

Finally, guest contributor John Poff of Pearl Technology takes us through the basics of anticipating and protecting against cyber attacks. John explains that, even though the computer systems containing your confidential business information are constantly being probed for security vulnerabilities, simple proactive measures can prevent the loss of your valuable digital property.

We would also like to invite you to a free educational seminar presented by our Business and Commercial Litigation Group, which will focus on the pitfalls associated with obtaining and protecting customers' credit card information. Several recent high profile cases involving thefts of this information makes this a topic of concern to all businesses that perform credit card transactions. Please join us on Tuesday, July 30 at noon in our Peoria office or via webinar.

Finally, if there are particular topics that you would like us to discuss in future editions, we welcome your recommendations. If we can assist you with these or any other legal matters, please do not hesitate to contact us at any time.

John P. Heil, Jr.
Business & Commercial Litigation Practice Group

**John Heil** is heavily involved in commercial litigation and general tort litigation on behalf of area businesses. Prior to joining Heyl Royster, he served for eleven years as a trial attorney with the Cook County State's Attorney's Office.

## Lunch & Learn!

**Business & Commercial Litigation Seminar**

**The Risky Business of Accepting Credit Cards**

Does your business or organization accept credit card or debit card payments? If so, then you won't want to miss our next seminar "The Risky Business of Accepting Credit Card Payments." Regardless of whether you use a vendor to process payments, your organization is expected to satisfy certain PCI Data Security Standard (PCI DSS) requirements. John Poff, Director of Information Security at Pearl Technology, and Heyl Royster attorneys will discuss those requirements and offer insights into what your organization can do to limit liability associated with credit card transactions.

Please join us on **Tuesday, July 30, 2013 from noon to 1:00 p.m.**

This free seminar will be offered **via webinar** and **in person** at the offices of

Heyl, Royster, Voelker & Allen
Suite 600, Chase Building, 124 S.W. Adams Street,
Peoria, IL 61602.

Lunch will be provided to those attending in person.

You may register by e-mail to sgullette@heylroyster.com or by phone at 309-676-0400 ext. 277.
We hope to see you there.

## CONTRACT CONSIDERATIONS BEFORE SHARING COMPANY INFORMATION WITH THIRD PARTIES

**By: Stacy Crabtree**
scrabtree@heylroyster.com

Companies receive, create, and store a wide range of information, some of which is proprietary and some of which could be subject to privacy laws and other statutes or regulations. As a result, it is important for companies to make sure that their information is protected and handled appropriately when placed into the hands of a third party vendor or service provider. Too many times, companies entrust their information to third parties relying on goodwill or the reputation of the third party without exercising further due diligence. Companies are often surprised to learn that the contracts they signed with the third parties really offer inadequate or possibly even no protection for their information. This article will discuss some contractual protections your company should consider when sharing information with a third party.

### A. Ownership

Due to the value of certain information to companies, information should be treated as an asset, meaning companies should protect their information by preventing third party claims of ownership. One of the basic ways to protect ownership of information is to include contractual provisions stating as such. This is especially vital in a situation where the third party vendor or service provider will be processing and/or creating additional information based on a company's proprietary information or ideas. Due to intellectual property laws, the creator of certain information may automatically have a right of ownership or interest in such information. So, it is important that companies are proactive in their contracts with third parties and identify what information they expect to own at the end of the relationship.

### B. Confidentiality

One of the most popular contractual provisions used in protecting information is a confidentiality clause or stand alone confidentiality agreement. These are not one-size-fits all, however. First and foremost, these clauses often differ in what constitutes confidential information subject to protection. Some agreements may require information to be marked as "confidential" in order to be subject to protection. This marking requirement poses a problem for companies that are not in the habit of marking confidential information as such and poses a problem for information that is provided verbally. In other agreements, the definition of confidential information may be limited only to a specific document, software program, or subject matter, and as a result, other company information that genuinely is proprietary is not protected. So it is critical that the definition of confidential information is closely scrutinized so ensure it covers what will actually be provided to the third party.

Secondly, confidentiality agreements typically differ in what is considered exceptions to the obligation of confidentiality. Generally, there should be exceptions to confidentiality requirements such as information that is already in the public eye (through no fault of the third party vendor, of course) and information that must be disclosed by law. In other words, if a company has already made certain information public, then the third party should not be obligated to hold that information in confidence. While on one hand not all agreements will include these exceptions, on the other hand we see agreements that include very broad and ambiguous exceptions. For example, we often see exceptions for information that is "independently created" by the third party. It is difficult to comprehend, though, what it means to be "independently created" in some situations where the information is created by the same person(s) that handled confidential information. We all know that it is not possible to unlearn something.

Some other ways confidentiality agreements may differ include the level of protection required, the allowable use of the confidential information, the time period for which the information must be protected, and the return or destruction of any confidential information

when the relationship with the third party ends. Depending on the goods or services provided by the third party and the nature of the information provided to the third party, the amount of protection required and other aspects of these confidentiality requirements may change.

**C. Information Security**

In addition to the above mentioned considerations, it is important that companies consider what information security requirements should be met by third parties collecting, storing, and/or processing confidential information, including personally identifiable information. Personally identifiable information is generically defined as information that can be used to identify a person, such as name, address, email, social security number, phone number, etc. Companies often collect this information for their customers and use third parties to process the information and store it. Poor information security controls by the third party vendor or service provider, however, increase the risk of a security breach and therefore the risk of an unwanted disclosure of customer information. Such disclosure may trigger significant fines and penalties under various states' privacy laws and require a significant amount of time and resources remedying the effects of the disclosure, including reputational harm.

Certain information security requirements may be legally required of companies and their third party vendors, whether by statute or contract. For example, the Heath Insurance Portability and Accountability Act (HIPAA) requires companies that are using a third party to collect or store protected health information enter into a Business Associate Agreement which includes an obligation that the third party abide by certain HIPAA security requirements. Similarly, when a third party will be handling credit card information, an obligation to follow PCI requirements should be considered. Companies may also desire the ability to audit the third party's security controls. Ultimately, whether it is a certain type of information security standard, compliance with a certain law, or a right to audit, companies should ensure their agreements meet their information security needs and satisfy any legal requirements.

**D. Limitations of Liability**

A final point, but very important one, pertains to limitations of liability in agreements. Many agreements include clauses that impose limitations on one party's potential liability to the other party. These clauses can prevent a third party vendor or service provider from being liable for certain types of damages such as consequential damages or lost profits, and can limit the dollar amount that the third party vendor or service provider can be liable for to the companies they are servicing. In fact, some agreements may state that the third party cannot be liable for any damages whatsoever. Therefore, even if a company is provided with the ownership, confidentiality, and information security protections it desires, those protections may be meaningless if there is little to no liability of the third party in the event of a breach.

In conclusion, prior to providing company confidential information (including personally identifiable information) to a third party, it is important to assess the nature of the relationship including what information the third party actually needs, the sensitivity of the information that will be provided, and any applicable legal requirements, and then engage an attorney to make sure the agreement adequately meets the company's needs. One word or phrase can make all the difference in an agreement, and no company wants that difference to be one that costs it its reputation, competitive advantage, goodwill, or bank account.

**Stacy Crabtree** represents clients in commercial and contract law, as well as tort litigation. Her clients include businesses large and small, and she regularly works onsite with a Fortune 50 manufacturing company assisting with vendor agreements, open-source software and freeware licenses, and compliance issues.

## INFORMATION SECURITY CONTROLS HELP PREVENT BREACHES

**By: John Poff, Director of Information Security, Pearl Technology**

As I began to write this article, like an old sports injury, there was one question that kept bubbling up to the surface demanding my attention: "What is the true information security risk to my business and what can I do about it?" I understand most of you probably have better things to do with your time than read this article in its entirety, so I've given you this "executive summary."

The reality of the situation is that if your business owns and operates a website, email server or provides any other service that's connected to the internet, then rest assured that service is under constant attack. The good news is that only a fraction of those attacks will result in a security breach, and that most breaches could have been avoided by simply testing ahead of time. If you want citations or references proving this statement, well, for that, you'll just have to keep reading.

Let's quickly talk about defining two terms that sometimes carry very different meanings in the information security world. Those terms are "Security Breach" and "Security Attack." For the purpose of this article, I'll use the ISO 27001 standard to define a security attack. "A security attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset." (ISO27001, 2005) On the other hand, a security breach is the intentional or unintentional release of secure information to an untrusted environment. (Privacy Rights Clearinghouse) Now that we got that out of the way, let's continue.

Every business that has an online presence like a website or email server is being attacked every second of every minute of every day on the internet. (Ponemon Institute, 2012) The most common types of attacks are simple, automated programs that scan every device connected to the internet looking for a vulnerability to exploit. Imagine if you will, a house thief wandering your neighborhood, checking every front door to see if it's locked. If one of them happens to be unlocked, he enters, steals some stuff, then moves on to the next house. If the door is locked, he simply ignores that house because he knows that there is an easier target down the street. Now, multiply that story by the internet. What we see is that it's not just one thief, one neighborhood, but hundreds, thousands, even millions of thieves wandering EVERY neighborhood in the world. Pretty scary thought, eh? Now before you go accusing me of fear mongering, throw up your hands and utter profanities about how I am wasting your time, I implore you to look at the positive side. If what I say is true, that your business is being attacked this often, then you should feel very good that your business hasn't had a security breach yet! (I'm assuming you haven't had a breach)! I can also tell you that only a fraction of internet attacks result in actual security breaches. In fact, according to the 2013 Verizon Data Breach Investigations Report, 3 out of 4 breaches were a result of this type of opportunistic attack and most businesses could have avoided the breaches by some very simple information security investments.

So, if three out of four security breaches are a result of opportunistic attacks, the question every business owner should be asking is, "What can I do to prevent my business from becoming one of these statistics?" Luckily, that answer is pretty simple. The Verizon Report goes on to recommend that a business implement a few security controls to help prevent these types of security breaches:

1. Eliminate unnecessary data and understand what is left.

   Figure out what kind of data your company has and what kind of information your company needs by conducting a data classification audit, or risk assessment. Depending on the size of your business, this could be as little as a few hundred dollars.

2. Ensure essential controls are met and regularly checked.

   This can be accomplished by regularly testing your systems through vulnerability scanning and penetration testing. A typical vulnerability scan for a small business is about five hundred dollars.

3. Evaluate the threat landscape of your business to prioritize a treatment strategy. Don't buy into a "one-size fits all" approach to security.

   It's generally free to have an initial consultation meeting with a cyber-security professional. I encourage every business owner to call up a qualified professional and ask them some questions. A good indicator that an individual or organizations are cyber security professionals is if you see certifications like CISM, CISSP, or CEH.

As you can see, securing your organizations information assets doesn't have to be expensive and complicated; in fact, there is an old saying in security: "Complexity is the enemy of security." It's been my experience that the most secure organizations are ones that first and foremost decide to do something about information security and then take simple, small steps towards achieving that goal. I believe the information in the Verizon Data Breach Investigations Report supports that observation.

**John Poff** is the Director of Information Security at Pearl Technology and has been working in Information Security for more than 10 years. He is a Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP) and Certified Ethical Hacker (CEH). He also acts as the Chief Information Security Officer for a number of organizations that range in size from $35 million to $2.4 billion in annual revenue.

## Protect Your Business - The Three Component Test for Restrictive Covenants in Employment Contracts

**By: Mark McClenathan**
mmcclenathan@heylroyster.com

Businesses often include restrictive covenants in employment contracts for the protection of business interests. Business interests can include the protection of client lists, trade secrets, confidential information, good will and market share. Employers generally achieve these goals by restricting an employee's conduct after employment by imposing non-competition clauses, non-solicitation clauses, and confidentiality provisions in their employment contracts. These provisions are called "restrictive covenants." Employers (and employees) need to be informed about the validity of restrictive covenants and recent trends in the courts regarding standards for restrictive covenants in order to be able to protect their respective interests.

***Reliable Fire Equipment Company v. Arredondo***

In December 2011, the Illinois Supreme Court clarified a long standing confusion regarding the standard for determining the validity of restrictive covenants in employment contracts in a case called *Reliable Fire Equipment Company v. Arredondo*. Reliable was in the business of selling and installing fire suppression equipment. Arnold Arredondo and Rene Garcia were employees for Reliable. While working at Reliable, Arredondo and Garcia created a new business which would be in direct competition with Reliable. However, Arredondo and Garcia both signed restrictive noncompetition agreements while employees at Reliable in which they agreed not to: (1) compete with Reliable during or one year after their employment in Illinois, Indiana, and Wisconsin; or (2) solicit sales or referrals from Reliable's customers. Arredondo resigned and Garcia was fired as a result of starting the new company. Reliable then sued Arredondo, Garcia, and the new company alleging a breach of their noncompetition restrictive covenant.

## Email Newsletter Available

Would you like to receive the newsletter electronically? Just send an email request to newsletters@heylroyster.com. You'll be able to enjoy the most cost-effective, environmentally-friendly way of receiving our business and commercial litigation news!

Because of a multitude of conflicting appellate court decisions attempting to tackle the job of whether to enforce a wide variety of restrictive covenants, the Illinois Supreme Court finally decided to clarify and set standards for restrictive covenants in employment contracts for the State of Illinois.

The Court re-established a three component test of reasonableness to determine the validity of restrictive covenants. A restrictive covenant will be upheld in Illinois if the restraint:

- is no greater than is required for the protection of a legitimate business interest of the employer;
- does not impose undue hardship on the employee; and
- is not injurious to the public.

The Court further went on to define a legitimate "business interest." Whether a legitimate business interest exists is based on the totality of the facts and circumstances of the individual case, including such factors as: near-permanence of customer relationships, the employee's acquisition of confidential information through employment, and time and place restrictions. However, these factors is not to be exclusive and are not to be weighed differently; rather, the importance of these factors are to depend on the specific facts and circumstances of each individual case.

In *Reliable Fire*, the lower courts previously held the restrictive covenant unenforceable claiming that Reliance did not have a legitimate business interest that justified the enforcement of the non-compete agreements. The Supreme Court reversed the decisions of the lower courts after re-defining the term "legitimate business interest" and sent the case back down to the lower courts to comply with the this new definition.

**Recent Application of the Clarified Restrictive Covenant Standards**

Many cases have applied the new *Reliable Fire* standard for restrictive covenants using the three component test. However, because the standard is fluent, and based on the totality of the facts and circumstances of each individual case, it is hard for employers or employees to predict the validity of restrictive covenants in employment contracts.

For example, in 2012, the Fourth District Illinois Appellate Court in *Zabaneh Franchises, LLC v. Walke*r, found a non-compete agreement in a tax firm's employment agreement enforceable. The employment agreement included a provision that restricted the employee from engaging, after termination of employment, in the business of tax preparation for any company client for two years and from soliciting or hiring company employees for one year in any competitive business. The court found that the tax firm had a legitimate business interest in imposing the restrictive covenants because of its customer relationships and its investment in developing the employee's skills. It further determined the employee's interests were protected in the restrictive covenant because the employee was only limited by not being able to prepare taxes for the clients that she serviced while an employee for the tax firm; thus her right to earn a living was not diminished. Therefore, the court upheld the restrictive covenant as reasonable.

An example of when a legitimate business interest has not been found enforceable is illustrated in the 2013 decision by the First District Illinois Appellate Court in *Gastroenterology Consultants of North Shore, S.C. v. Meiselman.* In that case, the court found that a employer did not have a legitimate business interest in imposing a restrictive non-compete provision in the physician's employment contract. The employer required that all doctors associated with the company sign a non-compete agreement which prohibited a doctor separated from the practice from soliciting or treating patients directly or in connection with any entity engaged in a competitive business located within 15 miles of each of the company's offices for a period of 36 months.

The court looked at the totality of the circumstances in making its determination, and found that *Gastroenterology Consultants of North Shore ("GCNS")* did not have a legitimate business interest in restricting the physician. The physician had his own patients and own referrals from physicians before working for the company, whom he still saw while working for GCNS. The physician also had his own independent relationship with his patients; billed his patients directly; and his compensation was

based on his independent practice, not GCNS's practice. The employer in this case only provided administrative support. The court held that GCNS did not have a legitimate business interest in need of protection by restricting the physician's practice after he left the company.

Also, in another 2012 decision, the Second District Illinois Appellate Court held that an otherwise "typical" non-competition and non-solicitation covenant in a salesman's contract was unenforceable, utilizing the *Reliable Fire* decision. In *Kairies v. All Line, Inc.*, the defendant employer was in the business of selling braided cords and rope, and employed Joseph Kairies as a salesman. Mr. Kairies signed a non-solicitation and non-competition agreement which restricted him from directly or indirectly soliciting any customer of All Line for two years after his termination. The agreement also restricted him from participating in the ownership, management, operation, or control of any business similar to the type of business conducted by All Line for two years.

The court determined the restrictive covenants in the All Line, Inc.'s contract to be invalid and unenforceable. The court determined that All Line did have a legitimate interest in protecting its company; however, the Court found the scope of the restrictive covenants too broad. First, the court held that the non-solicitation clause was too broad because it restricted Mr. Kairies from servicing any customer of All Line. A restrictive covenant on solicitation can restrict an employee from soliciting customers that the employee personally serviced, but generally an absolute bar on soliciting any customer is held unenforceable. All Line, Inc. could not restrict Mr. Kairies from servicing any and all customers of theirs.

Second, the court found the non-competition clause was too broad because it restricted Mr. Kairies from engaging in any activity for All Line's competitors. A non-competition covenant cannot restrict an employee from engaging in any employment position with a competitor, only employment that would harm the ex-employer. For example, a company cannot restrict an engineer from taking a janitorial job at a competitive firm. Thus, the court held that both restrictive covenants were too broad and overreaching to protect All Line's legitimate business interest, and thus, the Court held that the covenants were unenforceable.

For every case that exists where restrictive covenants are found enforceable, there is an equal number of cases where the covenant is not enforceable. There are numerous situations and issues that bear on a judge's decision, such as the reasonableness of the geographical scope of covenants, and how the courts define near-permanent relationships in determining the reasonableness of a restrictive covenant. Implementing restrictive covenants in employment contracts is essential to most businesses' survival; however, the uncertainty of the law makes it essential for the language in the restrictive covenants to be precise in order to meet the goal of a restrictive covenant, that is, to protect the business.

While the *Reliable Fire* decision was written to help guide business owners and their employees determine which restrictive covenants are enforceable and which are not, in reality, the waters are as muddy as they were before. Before drafting and implementing a restrictive covenant in an employment contract or signing an employment contract as an employee, we advise that you consult with an attorney.

**Mark McClenathan** concentrates his practice in commercial and civil litigation, including business and corporate law, construction law, and real estate. Prior to Heyl Royster, Mark worked in the legal departments of the Defense Logistics Agency of the Department of Defense, Land O'Lakes, Inc., and 3M Corporation.

**Heyl, Royster, Voelker & Allen**
**Suite 600, Chase Building**
**124 S.W. Adams Street**
**Peoria, IL 61602-1352**



## For More Information

If you have questions about this newsletter, please contact:

**Timothy L. Bertschy**
Heyl, Royster, Voelker & Allen
Suite 600, Chase Building
124 S.W. Adams Street
Peoria, IL 61602-1352
Phone (309) 676-0400 – Fax: (309) 676-3374
E-mail: tbertschy@heylroyster.com

**Peoria, Illinois 61602-1352**
Suite 600, Chase Building
124 S.W. Adams Street
Phone (309) 676-0400 – Fax (309) 676-3374

**Springfield, Illinois 62711**
3731 Wabash Ave.
P.O. Box 9678
Phone (217) 522-8822 – Fax (217) 523-3902

**Urbana, Illinois 61803-0129**
Suite 300, 102 East Main Street
P.O. Box 129
Phone (217) 344-0060 – Fax (217) 344-9295

**Rockford, Illinois 61105-1288**
PNC Bank Building, Second Floor
120 West State Street
P.O. Box 1288
Phone (815) 963-4454 – Fax (815) 963-0399

**Edwardsville, Illinois 62025-0467**
Suite 100, Mark Twain Plaza III
105 West Vandalia Street
P.O. Box 467
Phone (618) 656-4646 – Fax (618) 656-7940

**Chicago, Illinois 60603**
Suite 1203, 19 S. LaSalle Street
Phone (312) 853-8700

***www.heylroyster.com***