

CONTRACTS continued from page 1

debt until a judgment is received. Lastly, the Court will not order the debtor pay the costs associated with the litigation as the general rule is that each party bear its own litigation costs.

Not only will the litigation cost money, but the delinquent customer may even cost the business owner more money in the form of interest they had to pay to borrow money to keep their own vendors happy and their business afloat or even if the business owner did not have to borrow money, at the very least, they would be unable get the use of the money owed until it is paid by the debtor. So while they may have won the case, at the end of the day you must really ask did they really win?

What should have been done differently? Ideally you would have gotten paid up front but, as we all know, we don't live in an ideal world, so what is the backup plan? All business relationships be made and conducted in writing. If you can't afford not to get paid, make sure that the transaction is in writing - i.e., a contract.

A contract can be prepared that will help protect you against customers who do not pay. Along with the many concepts that need to be addressed in a contract, there are two that should be included. First, the contract should provide that, if the customer does not fulfill their obligations and you have to sue them, they must pay the costs of your attorney. Second, if payment is not received by you on the due date the outstanding debt will begin to accrue interest.

These are just two very common concepts that you should consider in any contract you enter into. There are many more concepts that should be addressed in your contracts. Which concepts and how they should be addressed are dependent upon what you are selling/buying, relative strength in negotiations between the parties, and the nature of your business. If you are unwilling or unable to write off the bad debt, it is a transaction that is important enough to warrant consulting with an attorney so that you will be protected in the event of a disagreement or the other side's failure to perform. To borrow from the old adage, an ounce of prevention may save you thousands of dollars later.

FRASCELLA & PISAURO, LLC.

ATTORNEYS AT LAW

100 Canal Pointe Blvd., Suite 209, Princeton, NJ 08540  
609-919-9500 Fax: 609-919-9510  
www.fplegal.com

*The contents of this newsletter is intended for informational purposes only and should not take the place of legal advice. Should you have any questions regarding this newsletter please call us at the numbers above.*

FRASCELLA & PISAURO, LLC.

ATTORNEYS AT LAW

Business News

Volume 1, Issue 1

July 2006

#### Introduction

Welcome to the first issue of Frascella & Pisauro, LLC.'s business law newsletter. It is my goal to produce at least two issues of this newsletter a year. Each issue will look at laws, cases or practice topics that directly affect your business. For example, in this issue, I look at a common issue left out of contracts that can cost your business thousands of dollars down the road; I examine NJ's new Identity Theft prevention Act and alert you to some proposed legislation working its way through Trenton.

I hope that you find this issue informative and useful. If you have topics that you would like to see discussed in future issues, please let me know. I would also appreciate any feedback you have on this issue. And, of course, if you do not want to receive future issues, please let me know by phone, mail or email at [busnews@fplegal.com](mailto:busnews@fplegal.com)

#### NEW JERSEY'S IDENTITY THEFT

Despite all the attention that identity theft has received lately, it is a crime which continues to grow at a rapid pace. It seems as though not a week goes by without hearing yet another news story about yet another company or governmental agency losing or having its data taken. Whether from educational institutions, financial institutions and even from the Veterans Administration, information regarding who we are is being taken at an alarming rate.

This growing problem is being addressed on both the state and federal level as states begin enacting laws and the US Congress has begun debating bill. As a business owner you should be aware of these actions and their potential impact on how you conduct your business.

New Jersey passed the Identity Theft Prevention Act, NJSA 56:11-44 et. seq which went into effect on January 1, 2006. The first section of the Act, which will not be explored in this article, addresses the rights of individuals whose identity has been stolen. The second section, which we will focus on here, is directed to the obligations of businesses and government in using and protecting the personal information in their control.

The section of the statute addressed to businesses is

#### HINDSIGHT AND FORETHOUGHTS ON CONTRACTS

There is a common misconception that most business owners seem to have regarding the collection of customer owed debts. Many times a business owner has come to me because their business is owed a couple of thousand dollars from a customer or two or more and they want to sue those customers in order to recover the money. The owner either cannot afford or is unwilling to write off the bad debt. Maybe they had to borrow money in order to meet their obligations under the contract; or perhaps, since the debtor has not paid, the business owner had to borrow money to cover expenses that would otherwise have been covered.

Sometimes there is no contract or after reviewing the contract, I have bad news for my client. Yes, the business owner has a good case. But that several thousand dollar debt will likely take several months or longer and may cost several thousand dollars in attorney fees to resolve in court – and that does not even take into account collecting on the judgment. The client is also not entitled to interest on the outstanding debt until a judgment is received. Lastly, the Court will not order the debtor pay the costs associated with the litigation.

Not surprising, we follow the American rule wherein each party pays its own costs associated with the lawsuit. Obviously, no business owner wants to hear that client is also not entitled to interest on the outstanding

further broken down into four parts. The first part describes *what a business has to do when its data has been taken or compromised*. The second part deals with the *destruction of data*. The third part sets *limits on the manner a business may use social security numbers*. Lastly, the fourth part outlines the *penalties for violating the statute*.

What is somewhat surprising is that the statute does **not** set forth standards for businesses to follow regarding the storage/protection of that data. The law does, however, direct the Division of Consumer Affairs and the Department of Banking and Insurance to develop regulations for implementing the statute. These regulations, which have not yet been proposed, will likely be the most important part of this statute and will likely set some guidelines for this.

Before we look any further into the subparts of this statute, let us first task, to whom does it apply and exactly what "personal" information must be protected? The statute applies to *any* business or governmental agency that keeps personal information on its customers/citizens or employees. The statute defines "personal information" as a **person's first and last name in conjunction with: Social Security Number; Driver's license number or State ID card number; or Account number, credit or debit card number with security code, access code or password**. Therefore, *any* entity that keeps *any* combination of the information listed above is subject to the statute.

Sections 11 and 13 of the statute provide guidance to business on *how* personal information can be used. Specifically, section 11 provides that when a business destroys the information in their possession they must do so in a manner that: "*make(s) it unreadable, undecipherable or non-reconstructable through generally available means..*"

At the very least, that means shredding paper records. What it means for electronic records is little murkier. While beyond the scope of this article, merely hitting the delete key on the computer really does not delete the information. The "deleted" information in fact can be easily retrieved. To truly delete the information so that it cannot be recovered requires additional steps and/or specialized software.

Section 13 sets forth how a business may use an individual's Social Security Number (SSN). According to the statute SSNs are the most frequently used method of identification in computer files. NJSA 56:11-45(g). A business cannot publicly post or display another's SSN in whole or in part (at least 4 or more numbers) or otherwise make the information available to the general public. For example, a business cannot place an SSN on a mailing to individuals unless otherwise required by law. SSNs cannot be used as ID numbers printed on cards (e.g., Health plan cards). Further, a company also cannot require a person to transmit their SSN over the Internet without having the proper security control in place.

In addressing a company's responsibilities when it suspects its data has been accessed, the statute first directs the company to report the theft/access to the Division of State Police in the Department of Law and Public Safety. After making the report, and unless instructed otherwise by law enforcement officials, the business must then notify its customers that their information has been taken. Obviously, this obviously can result in a public relations nightmare and, in some circumstances, can cause irreparable damages to the company.

There are various ways available to notify the victims. The first and most obvious of these is to send a letter. An additional primary method is to send an electronic notice that meets the requirements of the "Electronic Signatures in Global and National Commerce Act" 15 USC 7001. If the breach involves more than 500,000 persons and would cost the company more than \$250,000 to notify its customers than a company can use a substituted method of notification. Substituted notice consists of an email to the affected persons or businesses, a *conspicuous* notice on the company's website and a notification in a major statewide media.

Also if more than 1000 people are potentially impacted, the business must also notify all of the credit reporting agencies. §12g. Section 12 does have a "safe harbor" provision but I believe it may be a risky one to take. Section 12a provides that if the business determines that a breach has occurred but that the misuse of the data is not *reasonably possible* then the business does **not** have to disclose the breach to the customer. The decision that the data is not reasonably "misusable" must be made in writing and maintained by the company for five years.

Now that you have an understanding of what information must be protected and the ramifications of not protecting the data, what steps can a business take to protect the data? Although, as I mentioned earlier, guidelines should be forthcoming in the form of proposed regulations, aside from the technical aspects (which a good computer consultant should provide) the first and foremost line of defense is the company's employees. Unfortunately, since a significant number of thefts are caused by employees, they are also the most likely the *source* of any breach.

An employee's theft of data is not always the result of an intentional act. The VA employee whose laptop was recently stolen probably thought he was doing a good thing by bringing extra work home and what employer would complain about an employee who goes the extra mile! Unfortunately, he took home "personal information" and, when his laptop was later stolen, the personal information was stolen with it.

How many businesses allow, or at least do not prevent, their employees from taking work home with them? Once they leave the office, however, these laptops or thumb drives can be easily stolen or misplaced - perhaps when they stop to pick up milk or collect their children from daycare on the way home. Additionally, if the thumb drive is accessed on a home computer what happens if that home computer has been infected by viruses, spyware or other malware which then copies the data and transmits it to unauthorized users? The employee may not even know that their home machine is infected especially if they do not keep their anti-virus, anti-spyware and firewalls up to date, but the result is the same. The data has been compromised.

As the employer you are ultimately responsible for that data and you have several methods of protecting of your customers, employees and, therefore, your business. First, restrict access to the data to only those users who need access. Second, limit the time period that they can access that data - to only when it is needed. For example, if your business hours are 9-5 M-F eliminate your employees' ability to access the data on a Saturday or at 11 p.m. A competent computer consultant can configure your computers to accomplish this goal.

Just as important as finding the right technology to protect your data is having a policy in place covering the collection, usage and access to personal information. This policy should be in writing. It can be part of the company's employee handbook (you have a handbook, right?) or it can be a separate document. The policy should outline an employee's responsibilities regarding accessing the information and the manner and times which an employee can access it. It should limit the employee's ability to take the data off-site. The policy must also make it clear that any violations will result in disciplinary action - including firing. Such a policy may also have the added benefit of protecting your business by preventing an employee from taking the company's customer lists to a competitor.

Finally - once the policy is in place, the policy must be enforced!

All new hires and current employees should be screened to ensure that they do not have a criminal history or other background that might cause you to question their ability to be trustworthy. Lastly, you must monitor your employees. Are they accessing information that they should not? Are they taking home work that would be safer if it stayed at the office? Are they installing software on your machines that you did not approve? All of these activities are invitations to data theft and could mean a long expensive road for your business.

As you can see, the impact of identity theft has some very serious business implications. Failing to properly protect your customers' personal data leaves the business open for civil lawsuits by those customers whose identities have been stolen.

And nobody wants to hear from a lawyer.

*This article is based upon a presentation made to the Pennington Business and Professional Association in June 2006.*