

# Why Does the FACTA Law Matter to Schools?

**As an employer, what you don't know about FACTA Law can definitely hurt you.**

FACTA, stands for Fair and Accurate Credit Transaction Act. FACTA is the law creating a policy which allows any American access to their credit report once per year. The law went into effect Jan. 1, 2005. So what does that mean for you as an employer?

On June 1, 2005, a new portion of the FACTA law went into effect. It says that any employer (even if you only employ one person, and you have their personal information so that you can pay social security taxes,) whose action or inaction results in the loss of employee information, can be fined by federal and state government, and sued in civil court.

A USA Today article on the FACTA law from Jan. 14, 2005, stated "Bet you didn't know that." But you need to know, and need to know what procedures you can put into place to protect yourself.

## **Businesses affected by the FACTA law**

"A business that makes a mistake could bear the brunt of a regulation like this," says James Plummer, policy analyst at Consumer Alert, a non-profit group that focuses on a free-market approach to consumer regulations.

The USA Today article goes on to say that "if you don't shred and information gets out, there are penalties." But what if you do shred all potential employee information, and take all necessary procedures to protect your past, current, and future employees' identities, and the information still gets out somehow? Under the FACTA law, you could still be held responsible.

You may not think information theft could happen to you, but neither did this short list of companies, universities, government institutions, and businesses that have had employee or customer information stolen from them:

- DSW Shoe Warehouse
- TJX
- Hannaford
- California State University (Chico)
- University of California - Berkeley
- University of Texas
- Austin Department of Motor Vehicles
- Bank of America
- Choice Point
- San Antonio Marine Corp Reserve Center

## **How can you, as an employer, minimize your liability?**

There are hundreds of procedures you can take to reduce liability, which are probably things you already do. Document shredding, redaction of electronically stored information, careful screening of employees who will be coming into contact with personal information of customers and employees, physically locking file drawers with sensitive information, and setting up firewalls on computer equipment connected to the Internet, among hundreds of other solutions, are all good ideas. The old saying that an ounce of prevention is worth a pound of cure is definitely the case

when it comes to securing personal information. However, no matter what preventative procedures you put into place, there is no 100% effective way to be sure that employee's information won't be compromised. Even if the information doesn't get out from your company, an employee can claim that it did.

That's a scary thought! What if an employee claims that their information was stolen through the actions of your company, but there's no real proof to back it up? You will end up hiring (or using) an attorney to represent and defend your company in court. At \$150 - \$200/hour for most attorneys across the United States, how long can you afford to defend your company?

### **So what can you do?**

The only sure solution, or at least the only solution that would at least provide an affirmative defense against the fines, fees, and lawsuits you could incur as an employer under the FACTA Law, is to offer some sort of Identity Theft protection policy as a benefit to your employees.

As an employer, you can choose whether or not to pay for this added benefit. However, the most important thing you can do is to make the protection available, and have a mandatory employee meeting, to help employees understand Identity Theft. Teach reasonable steps to take in reference to protecting sensitive information and explain the protection that you are making available to them. When you make the protection available, and include it as part of your employee training, and when your employees have been educated on the dangers of Identity Theft, they can either elect to have identity theft coverage as a benefit, or they can decline the coverage as a benefit.

If the employee has Identity Theft coverage and becomes a victim, it is beneficial to your business, because an employee with Identity Theft coverage will spend less time, less money, and will experience less frustration while trying to have their information restored. This will get them back on the job and focused on work more quickly.

If the employee declines the coverage, and later claims that the information was stolen as a result of you or your company's actions, you have a piece of paper, with their signature, saying that they attended the presentation, that the presentation is a part of the procedure you take when hiring any employee, and that the employee declined the coverage.

Choosing to not make Identity Theft coverage available leaves you exposed to a slew of costs under the FACTA law. They include making you responsible for: the unlimited dollar amount that you can be sued for under civil liability, federal fines of up to \$2,500.00 per employee per incident, and state fines of up to \$1,000.00 per employee per incident.

Recommended course of action? Have a benefits consultant who offers an Identity Theft protection plan present to your employees. Help them set up a 1 hour presentation with your employees. As a matter of company policy, make it mandatory that all employees attend. You want your employees to be protected from this awful crime. If they choose not to be, but you've given them the option of being protected as part of your normal training, then the liability becomes theirs, not yours, when they become a victim of identity theft.