Workforce Solutions

The Cost of Identity Theft to Business – What Business Owners Must Know Now

An Introduction to the Fair and Accurate Credit Reporting Act (FACTA): What Business Owners Must Know Now

It often seems that there isn't a week that goes by that we don't learn that hackers have managed to breach corporate, government, or university databases in a major way. Entities ranging from ChoicePoint to the Department of Veteran's Affairs to the University of California, Los Angeles and the University of Texas School of Business have all been recent victims. The individuals whose personal information was compromised all share a common fear: that identity thieves will use their data, including phone numbers, social security numbers, and driver's licenses, or birth dates, to take out loans, open new credit card accounts, access bank accounts, or obtain long distance calling accounts or cell phones in their name.

There is very good reason to be concerned. According to the National Identity Theft Resource Center, of the approximately 44 million Americans who have been the victims of identity theft at some point, each spent an average of 600 hours and $1,495 getting their finances straightened out. And, that doesn't include attorney's fees.

The High Cost of Identity Theft to Business

While that's plenty to worry about, the cost of identity theft to business is even greater. Because a number of consumer protection laws help to limit the financial liability for the victims of identity theft, businesses wind up bearing the brunt of costs for account balances, goods, or services lost to identity thieves. In 2004, identity theft cost financial institutions and businesses an estimated $52.6 billion, according to the 2005 Javelin Identity Fraud Survey Report, published by Javelin Strategy & Research and the Better Business Bureau. There are also indirect costs to businesses such as lost productivity and allowing employees who are victims extra time off to resolve the identity theft.

In an effort to help fight what has become the fastest-growing crime in the U.S. – identity theft - Congress added new sections to the federal Fair Credit Reporting Act (FCRA) when it passed FACTA – The Fair and Accurate Credit Transactions Act of 2003. Privacy, limits on information sharing, new consumer rights to disclosure and accuracy are all addressed.

However, these new provisions also create serious new responsibilities – and potential liabilities – for businesses nationwide. Simply put, if data aiding an identity theft originates from a security breach at your company, you could be sued, fined, or become a defendant in a class action lawsuit by affected employees whose personal information has somehow gotten out. In this brave new world, not only do you have to worry about safeguarding your own personal information from identity thieves, you've got to worry about what could happen if another's personal information is stolen from your company and results in identity theft.

Ready or not, it's time to get familiar with FACTA, and develop a reasonable plan to reduce and mitigate potential risks as much as possible. For many small businesses, this could be as simple as having a sturdy, dependable shredder – and routinely using it - to far more sophisticated security measures for larger organizations that maintain extensive computer databases.

An Overview of FACTA

•FACTA was signed by President Bush on December 4, 2003.
•The provisions of the law have been

phased in over the past few years, and all are now in effect.

- Every consumer can get one free copy of their credit report each year at www.annualcreditreport.com or by calling 877-322-8228.
- Businesses must leave off all but the final five digits of a credit card number on electrically printed store receipts as of December 1, 2006.
- Employers must destroy all information obtained from a consumer credit report before discarding it.
- Consumers who suspect that they are the victims of identity theft only need to notify one of the three credit reporting services (Experian, TransUnion or Equifax) to initiate a nationwide fraud alert.
- Mortgage lenders must provide the credit score they use to determine a loan's interest rate, regardless of whether the loan is approved or denied.
- FACTA is enforced by the Federal Trade Commission (FTC).

Initially, legal analysts believed that FACTA applied only to the banking and financial-related industries. However, because it is basically impossible to be an employer in the 21st Century without collecting, disseminating, maintaining and destroying personal information, the current consensus is that if you have even one worker – a yard man, a nanny – and you obtain their personal information to pay Social Security taxes, you must not only safeguard that information while it is in your possession, you must "destroy" the information before you throw it away. The law requires

the "shredding or burning" of all paper and the "smashing and wiping" of all computer discs containing personal information "derived from a consumer report" before they are thrown away.

Who Does FACTA Affect?

This law applies to any business, regardless of size, that collects personal information or consumer reports about customers or employees to make decisions within their business(including names, credit card numbers, birthdates, home addresses and more). Covered entities include:

- Employers – including individuals
- Insurers
- Lenders
- Mortgage brokers
- Landlords
- Automobile dealers
- Attorneys
- Debt collectors
- Private investigators
- Tax preparers
- Financial Advisors and Credit Counseling Services
- Investment or financial advisory services, including instruction on individual financial management and tax planning

Reasonable Measures of Destruction

According to the Federal Trade Commission, reasonable measures include:

- Burning, shredding, or pulverizing documents so they become impossible to put back together or read.
- Erasing media files or electronic files that contain any consumer reports so that they cannot be reconstructed or recovered.
- After reviewing company practices to ensure that they are reasonably designed to protect personal information, some are also hiring outside sources that specialize in destroying personal records. There are currently about 2.000 companies in North America that provide records destruction services; approximately half of them do it as their primary business.

Penalties

If personal information isn't destroyed and it gets out, FACTA provides penalties including:

- Civil liability. An employee could be entitled to recover actual damages sustained if their identity is stolen from an employer. Or, an employer could be liable for statutory damages for up to $1,000 per employee.
- Class action lawsuits. If large numbers of employees are impacted, they may be able to bring class action suits and obtain punitive damages from employers.
- Federal fines. The federal government could fine a covered business up to $2,500 for each violation.

Now What? It's Time to Develop a Plan!

The Federal Trade Commission (FTC) has created a new Division of Privacy and Identity Protection to focus on aggressive enforcement of identity theft cases. In order to comply with FACTA, Betsy Broder, the Assistant Director of that FTC division, was quoted in the March 2006 American Bar Association Journal saying that means businesses need to have a written plan describing how customer data will be safeguarded and a staff member or company officer designated to be responsible for implementing that plan. Broder went on to say, "We're not looking for a perfect system. But we need to see that you've taken responsible steps to protect your customers' information."

Many large companies will entrust such planning and execution to a chief technical officer or a chief privacy officer. However, Broder says she understands that small businesses cannot be expected to hire a full-

time privacy specialist, but added that all businesses must be able to show that they have a security plan in place. In other words, effort counts.

According to the FTC, a "reasonable" plan to safeguard personal information includes:

- Designating an employee (or employees) to coordinate and be responsible for the security program.
- Identifying "material internal and external" risks to the security of these personal data (with such a risk assessment including employee training on the detection, prevention, and response to attacks or other system failures).
- Designing and implementing reasonable safeguards to control the risks identified in the risk assessment.
- Continually evaluating and adjusting the security plan in light of the results of ongoing monitoring and testing of the program, material changes to business arrangements, or to the company's operations, or "any other" circumstances that could have a material impact on the effectiveness of the security plan.
- Creating a mitigation plan. Even with the FTC's focus on "reasonable" security measures and "appropriate" risk levels, there is still the real possibility that security breaches may occur, regardless of what precautions are taken. This mitigation plan should kick in when there is a privacy or security breach and there is a need to "repair it" immediately in the eyes of customers, government regulators, and management.

Remember: perfection is not the goal here; the standard is one of "reasonableness." A sensible and effective program will go a long way towards reducing the risk of federal government enforcement, even if the security policy should fail in a particular situation and a security breach results.

Some Steps to Take Right Now

Even if you are a very small employer, there are some proactive measures you can take immediately, in both your personal and business lives.

• Burn or shred, with a confetti or cross-cut shredder, any financial papers, mail, or credit reports that contain personal information. NEVER RECYCLE SUCH DOCUMENTS!

• Call 1-888-5OPTOUT and request credit card companies to stop sending pre-approved credit card applications to your home or business. These are ticking identity theft time bombs.
• Also ask your credit card company to stop delivering so-called "convenience checks" to your home and business. These, too, are time bombs.
• Invest in a durable cross- or confetti-cut shredder. Simple strip-cut shredders are no longer sufficient. Look for strength – can the shredder cut through credit cards, data CDs, diskettes, and staples?
• Many shredders have to be turned off to cool down after shredding just a few pages. While that may be sufficient for most consumers, if you plan to destroy a great deal of business paperwork, a more durable model is in order. And, the more pages you can shred at once, the less time you'll waste destroying unwanted credit card applications and other documents containing personal information.
• Because it's impossible to tell what's real and what's fake online, delete any e-mail that asks for personal information and instruct your employees to do the same.
• Hang up on telemarketers, especially those who seem to be digging for personal information – yours or your employees. Instruct your employees to do likewise.
• Limit the number of credit cards you hold, both business and personal. Religiously review your financial statements monthly and instruct your employees to do the same. The sooner you discover an incident of identity theft, the better.

Conclusion

The law of identity theft has changed dramatically in the past year, and many believe these changes will continue and expand. Undoubtedly, security risks will remain because of the huge volume of personal data that is collected, disclosed, and used on a daily basis in the United States. The most important steps you can take right now include an awareness of the increasing legal obligation arising from identity theft risks, and establishing reasonable security practices to protect the personal information in your possession.

For additional information, visit the FTC's website at www.ftc.gov or call toll-free 1-877-FTC-HELP (1-877-382-4357). You may also visit:
www.texasworkforce.org, click on "Businesses and Employers," and under "Publications," you'll see Back Issues of Texas Business Today. Visit the Fall 2005 issue to see "Identity Theft in the Workplace: What You Must Know".

Information contained in this report can be found in the Texas Workforce Commission's book, *Especially for Texas Employers.*