

**AN INTRODUCTION TO FACTA
(FAIR & ACCURATE CREDIT REPORTING ACT)**

by Linda Carter

© The Retail Management Advisors, Inc.

email: LC@the-retail-advisor.com

Identity Theft is a serious crime with serious consequences for both the consumer and the business. The following information was taken from “Texas Business Today” published by the Texas Workforce Commission.

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 does not include attorney’s fees.

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.** This is according to the 2005 Javelin Identity Fraud Survey Report published by Javelin Strategy & Research and the Better Business Bureau. In addition, there are indirect costs to businesses such as lost productivity and allowing employees who are victims extra time off to resolve identity theft.

Identity Theft is the fastest growing crime in the United States. In order to help fight it, Congress has added new sections to the federal Fair Credit Reporting Act (FCRA) when it passed FACTA in 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 in the United States. 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 people (employees or customers). *This means, that as a business owner you not only have to be concerned with people getting your personal information, but you must also worry about what could happen if another’s personal information is stolen from your company and their identity is stolen.*

- ▶ 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. There are three major credit reporting companies in the United States. One way to get your free credit reports so you are looking at your credit every 4 months throughout the year is to order one from each agency each 4 months. Since they all share information it is likely that what you find on one will be on the others.
- ▶ 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. If your credit card equipment is not yet doing this, it is time to get it changed NOW. This may mean upgrading your company’s software.
- ▶ Employers must destroy all information obtained from a consumer credit report before discarding it.

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, birth dates, home addresses and more). Retailers are covered as:

- ▶ Employers
- ▶ Lenders (for a retailer, this would be those who have in-house charge accounts)

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. Strip shredders are not good enough; it needs to be a cross-cut shredder.
- ▶ Erasing media files or electronic files that contain any consumer reports so that they cannot be reconstructed or recovered.

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 any be able to bring class action suits and obtain punitive damages from employees.
- ▶ 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!

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.

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 arrangement, 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.

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 our 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?

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.

© The Retail Management Advisors, Inc., All Rights Reserved
510 Red Oak, Allen, TX 75002
Phone: 877-206-1299