

# Personal Data Loss Can Impact Your Bottom Line

*What FACTA means for your business*

What's your first thought when someone mentions identity theft? "It's a consumer issue and has nothing to do with my business," is what we commonly hear. Nearly 18% of identity thefts, with known breaches, occurred at work. (Identity Theft Resource Center) The Federal Trade Commission reports that in 2004, Illinois was ranked #10 in "Identity Theft Victims by State."

What does this mean for your business? On June 1, 2005, the Disposal Provision of the "Fair and Accurate Credit Transactions Act" (FACTA) went into effect. Any business that collects and stores any personal information from clients to employees will be punished if the information is lost or stolen. There are

federal fines of up to \$2,500 and state fines up to \$1,000 per person, per incident plus the liability for any damages individuals suffer as the result of information breaches.

In the first half of 2005 alone, businesses reported over 50,000,000 consumer information data breaches. That's astounding considering only 10 states require security breach notifications. According to USA Today, Jan. 14-16, 2005, the average individual identity theft loss is \$92,893 and 600 work hours to clear the issue. Imagine the consequences to your business if just 10 of your employees' records are violated or claim to be violated. FACTA makes no allowances if you can't prove otherwise. In civil and class action lawsuits, federal and

state fines could reach up to \$35,000 and over \$900,000 and 600 work hours per employee. At \$150-200 an hour for an attorney, how long can you afford to defend your business?

Prevention is great but not a guarantee. Offering employees an identity-theft protection benefit with ongoing background monitoring provides additional defense. Ongoing monitoring is an early warning system where employees can call on experts to correct problems immediately. This saves time and limits the losses that employees may incur because of an information breach. This also saves you costs associated with employees' frustration and inability to pay attention at work. The

benefit can be offered as a voluntary benefit with no cost to the employer, as an employer-paid fringe benefit, or a combination of both. Choose a service provider that offers identity restoration as part of the service. However, look out for companies that provide a false sense of security and only produce a do-it-yourself kit.

Identity theft is something every business should take seriously. By helping to protect your employees' identity, you help protect your business from diminished employee productivity and potential liability.

**Terrance and Alissa Nolan,**  
Employee Benefits Consultants



## HOW ARE YOUR SALES DOING?



**Marketing Strategies** that help you understand your customer and why they BUY.

Call TODAY for FREE initial consultation. What do you have to lose? **CUSTOMERS!**



**We turn Leads into Sales and Sales into Profit**

Roneida J. Martin, President  
**847-302-1367**  
[www.pursuitofprofits.com](http://www.pursuitofprofits.com)

### *Some helpful steps that may minimize your liability*

- Store sensitive personal data in secure computer systems or locked file cabinets.
- Limit access to qualified/trained personnel.
- Enforce strict penalties for illegitimate browsing and access.
- Dispose of information properly; cross-cut shredding, "wiping" electronic files, destroying disks & CDs.
- Conduct regular staff training, of all employees and contractors.
- Put limits on data collection, data display and disclosure of sensitive information.
- Do not use the SSN as customer, employee or health insurance ID number.
- Conduct background checks on employees, cleaning / temp services and contractors.
- Notify individuals of computer security breaches involving sensitive personal information.
- Develop a crisis management plan to be used if sensitive data is lost or stolen.