

# IDENTITY THEFT: YOUR OBLIGATIONS UNDER FACTA, HIPAA & GRAMM-LEACH-BLILEY

Identity Theft Risk Solutions

## Non-Public Information Your Responsibility

Kurt Schwamberger  
[kurt@IDTrisksolutions.com](mailto:kurt@IDTrisksolutions.com)  
616-855-4270



---

---

---

---

---

---

---

---

### Today's Topics

- ♦ What identity theft is in reality
- ♦ Laws related to identity theft that affect employers, executives and business owners

---

---

---

---

---

---

---

---

### Who Is Being Held Responsible

*"A rise in identity theft is presenting employers with a major headache: They are being held liable for identity theft that occurs in the workplace."*

Douglas Hottle, Meyer, Unkovic & Scott,  
"Workplace Identity Theft: How to Curb an HR Headache"  
BLR: Business and Legal Reports, September 19, 2006

---

---

---

---

---

---

---

---

# IDENTITY THEFT: YOUR OBLIGATIONS UNDER FACTA, HIPAA & GRAMM-LEACH-BLILEY

## Identity Theft Prevalent at Work

*"With the workplace being the site of more than half of all identity thefts, HR executives must 'stop thinking about data protection as solely an IT responsibility,' says one expert. More education on appropriate handling and protection of information is necessary, among other efforts."*

*"ID Thefts Prevalent at Work", Human Resource Executive, April 5, 2007*

---

---

---

---

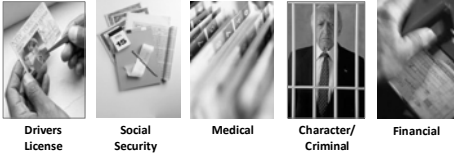
---

---

---

---

## Five Common Types of Identity Theft



---

---

---

---

---

---

---

---

## The Cost to Businesses

- Employees can take up to **600 hours, mainly during business hours**, to restore their identities
- "If you experience a security breach, 20 percent of your affected customer base will no longer do business with you, 40 percent will consider ending the relationship, and 5 percent will be hiring lawyers!"\*
- "When it comes to cleaning up this mess, companies on average spend **1,600 work hours per incident** at a cost of \$40,000 to \$92,000 per victim."\*

\*CIO Magazine, *The Coming Pandemic*, Michael Freidenberg, May 15<sup>th</sup>, 2006

---

---

---

---

---

---

---

---

# IDENTITY THEFT: YOUR OBLIGATIONS UNDER FACTA, HIPAA & GRAMM-LEACH-BLILEY

## **Ask Yourself This Question**

Why should all businesses, corporations, schools, financial institutions, hospitals and governmental bodies be concerned about identity theft, FACTA-Red Flag Rules, GLB Safeguard Rules, and state legislation?

**Answer: Liability, both civil and criminal.**

---

---

---

---

---

---

---

---

## **Important Legislation**

- ◆ FACTA and FACTA Red Flag Rules
- ◆ Fair Credit Reporting Act
- ◆ Gramm, Leach, Bliley Safeguard Rules
- ◆ HIPAA
- ◆ Individual State Laws

---

---

---

---

---

---

---

---

## **Fair and Accurate Credit Transactions Act (FACTA)**

This law applies to businesses and individuals who maintain, or otherwise possess, consumer information for a business purpose and requires businesses to develop and implement a written privacy and security program.

Employee or customer information lost under the wrong set of circumstances may cost your company:

- ◆ Federal and State fines of \$2500 per occurrence
- ◆ Civil liability of \$1000 per occurrence
- ◆ Class action lawsuits with no statutory limitation
- ◆ Responsible for actual losses of an individual (\$92,893 Avg.)

---

---

---

---

---

---

---

---

# IDENTITY THEFT: YOUR OBLIGATIONS UNDER FACTA, HIPAA & GRAMM-LEACH-BLILEY

## **FACTA Red Flag Rules**

Red Flag Rules recently became effective in January 2008, and compliance is required by November 2008. Under these rules, covered accounts, creditors and businesses:

- Must develop and implement a written privacy and security program.
- Must obtain approval of the initial written program from either its board of directors or an appropriate committee of the board of directors.
- Or if the business does not have a board of directors it must have a designated employee at the level of senior management. Small businesses are not exempt.
- The oversight, development, implementation and administration of the program must be performed by an employee at the level of senior management.

---

---

---

---

---

---

---

---

## **FACTA Red Flag Rules**

These rules also provide that covered accounts, creditors and businesses must also ensure their service providers and subcontractors comply and have reasonable policies and procedures in place. The rules state:

- Liability follows the data.
- A covered entity cannot escape its obligation to comply by outsourcing an activity. Businesses must exercise appropriate and effective oversight of service provider arrangements.
- Service providers and contractors must comply by implementing reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft.
- Contractors with whom the covered accounts exchange PII are required to comply and have reasonable policies and procedures in place to protect

---

---

---

---

---

---

---

---

## **Fair Credit Reporting Act (FCRA)**

If an employer obtains, requests or utilizes consumer reports or investigative consumer reports for hiring purposes/background screening, then the employer is subject to FCRA requirements.

[www.ftc.gov/os/statutes/031224fcra.pdf](http://www.ftc.gov/os/statutes/031224fcra.pdf)

---

---

---

---

---

---

---

---

# IDENTITY THEFT: YOUR OBLIGATIONS UNDER FACTA, HIPAA & GRAMM-LEACH-BLILEY

## **Gramm, Leach, Bliley Safeguard Rules**

Eight Federal Agencies and any State can enforce this law

This law applies to organizations that maintains personal financial information regarding its clients or customers

**Non-Public Information (NPI) lost under the wrong set of circumstances may result in:**

- ◆ Fines up to \$1,000,000 per occurrence
- ◆ Up to 10 Years Jail Time for Executives
- ◆ Removal of management
- ◆ Executives within an organization can be held accountable for non-compliance both civilly and criminally

Be Sure To Check With Your Attorney On How This Law May Specifically Apply To You

---

---

---

---

---

---

---

---

## **Privacy and Security Laws**

**These laws require businesses to:**

- ◆ Appoint, in writing, an Information Security Officer
- ◆ Develop a written plan and policy to protect non-public information for employees and customers
- ◆ Hold training for all employees
- ◆ Oversee service provider arrangements

---

---

---

---

---

---

---

---

## **Protecting Personal Information A Guide For Business**

This FTC publication suggests that companies should:

- ◆ **“Create a culture of security by implementing a regular schedule of employee training”** (pg 17)
- ◆ **“Make sure training includes employees at satellite offices, temporary help, and seasonal workers.”** (pg 17)
- ◆ **“Ask every employee to sign an agreement to follow your company’s confidentiality and security standards for handling sensitive data”** (pg 16)



---

---

---

---

---

---

---

---

# IDENTITY THEFT: YOUR OBLIGATIONS UNDER FACTA, HIPAA & GRAMM-LEACH-BLILEY

## Protecting Personal Information A Guide For Business

*"Before outsourcing any of your business functions – payroll, web hosting, customer call center operations, data processing, or the like – investigate the company's data security practices . . ." (pg 19)*

**Your liability follows your data . . .**



---

---

---

---

---

---

---

---

Betsy Broder: The FTC will act against companies that don't protect customers' data.



*"We're not looking for a perfect system," Broder says. "But we need to see that you've taken reasonable steps to protect your customers' information."*

- "Stolen Lives", ABA Journal, March 2006

---

---

---

---

---

---

---

---