

Identity Theft - FTC Guidance* for Protecting Personal Information

Presented on October 16, 2008 to the



Rotary Club of Conshohocken-Plymouth-Whitemarsh

By: **Robert A. Listerman, CPA, CITRMS****

**Certified Identity Theft Risk Management Specialist

* Portions adopted from the Federal Trade Commission's
"Protecting Personal Information Guidance for Business"

Disclaimer

- *The laws discussed in this presentation are, like most laws, constantly amended and interpreted through legal and social challenges. You are encouraged to review the laws and draw your own conclusions through independent research.*
- *Presenter is not an attorney, and the information provided is not to be taken as legal advice.*

Data Breaches Threaten You

Number of Reported* ID Breaches:

- 2005 - 158 reported affecting 64+ million
- 2006 - 312 reported affecting 19+ million
- 2007 - 448 reported affecting 127+ million
- 2008 - 524 reported affecting 30+ million, 10/07/08
- Since 2005 – Over 1,442 reported incidences
- Since 2005 – Over 240+ million affected, 10/07/08

* Source: **Identity Theft Resource Center**

Data Breaches Threaten You

2007 Breaches by Category of Source Aggregator

Category	# Incidences	# Record
Financial Inst.	31	8,834,476
Business	131	105,545,469
Educational	111	1.184,575
Gov/Military	110	8,156,682
Medical/Healthcare	65	3,997,133
Total	448	127,718,335

Five Common Types of Identity Theft



**Drivers License
Identity Theft**



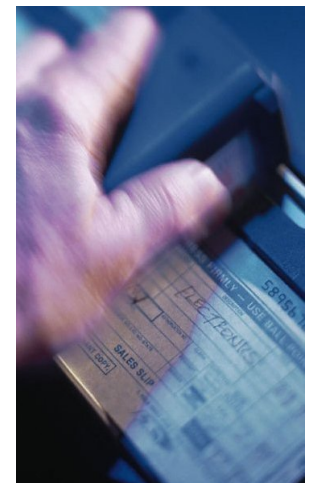
**Social Security
Identity Theft**



**Medical
Identity Theft**



**Character / Criminal
Identity Theft**



**Financial
Identity Theft**

Identity Theft is not just about Credit Cards!

The Cost to Your Business

- *Employees can take up to 600 hours, mainly during business hours, to restore their identities*
- *“If you experience a data breach, 20% of your affected customer base will no longer do business with you, 40% will consider ending the relationship, and 5% 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.”**

Responsibilities of Data Keepers

“All companies that engage in financial transactions are bound by law to establish and enforce information security programs to prevent identity theft.”

Judith M. Collins. Preventing Identity Theft in Your Business : How to Protect Your Business, Customers, and Employees. (Wiley, 2005). Page FM4.

Responsibilities of Data Keepers

- Why should all Businesses, School Districts, Financial Institutions, Governmental Agencies, Non-Profit Organizations and Hospitals be concerned about Identity Theft?
- Answer: **Liability, both Civil and Criminal**

Important Federal and State Legislation

- **FACTA**
- **HIPAA Security Rule**
- **Gramm, Leach, Bliley Safeguard Rules**
- **Multiple State Identity Theft Laws (Currently 42 States have adopted their own ID Theft Laws)**
- **The NCSL data breach legislation website can be accessed at:**
www.ncsl.org/programs/lis/cip/priv/breach.htm

F.A.C.T.A. (Fair and Accurate Credit Transactions Act)

Applies To Every Business And Individual Who Maintains, Or Otherwise Possesses, Consumer Information For A Business Purpose.

Employee, Customer or Vendor 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 Individual**

F.A.C.T.A. 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 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

F.A.C.T.A. 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 information.

FACTA Applies to:

- Workplaces that employ one or more people, accept credit cards, or buy or sell products or services over the Internet
- Workplaces that conduct credit checks or use, gather, or obtain consumer information
- Workplaces that store consumer reports and information
- Workplaces that destroy personal information

HIPAA Security Rule

Scope broadened on April 21, 2006

Applies To Any Organization Or Individuals Who Retain Or Collect Health Information.

Medical information lost under the wrong set of circumstances may result in:

- **Fines up to \$250,000 per occurrence**
- **Up to 10 Years Jail Time for Executives**

Gramm, Leach, Bliley Safeguard Rules

Eight Federal Agencies and any State can enforce this law

Applies To Any Organization That Maintains Personal Financial Information Regarding It's Clients, Customers, Employees, Vendors, and Prospective of each.

Non Public Information (NPI) lost under the wrong set of circumstances results 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**

Gramm, Leach, Bliley Safeguard Rules

Applies to Any Organization Including :

- *Financial Institutions**
- *School Districts*
- *Credit Card Firms*
- *Insurance Companies*
- *Lenders*
- *Brokers*
- *Car Dealers*
- *Accountants*
- *Financial Planners*
- *Real Estate Agents*

**The FTC categorizes an impressive list of businesses as FI and these so-called “non-bank” businesses comprise a huge array of firms that may be unaware they are subject to GLB.*

Gramm, Leach, Bliley Safeguard Rules & HIPPA

Require businesses to:

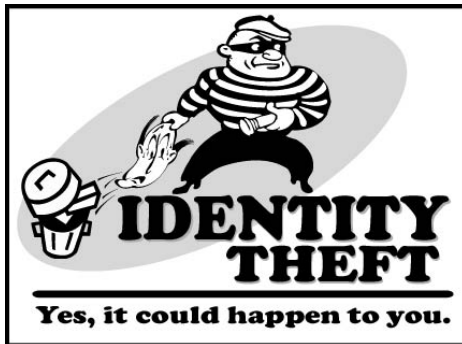
- **Appoint in writing an Information Security Officer**
- **Implement a written policy to protect Non-Public Information for employees and customers**
- **Hold mandatory training for employees who have access to Non-Public Information**

BTR-SECURITY

Identity Theft Protection, Detection & Restoration

Don't Think This Can Happen To You?

- If a thief steals a computer or files from your office with **Non-Public Information** of your employees or customers which leads to ID Theft, They and the federal government will hold you accountable.
- The first thing they probably will ask is what have you done to show good faith in being in compliance with the FACTA, HIPPA and GLB Safeguard Rules?
 - Have you held mandatory privacy & security compliance meetings?
 - Have you appointed a security officer?
 - Have you implemented a written Sensitive & Non-Public policy?
 - Have you made ID Theft Protection available to your employees?



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



The Federal Government has authorized the FTC to enforce these new laws.

The Employee Confidentiality Document

Acts as a **Good Faith** step in attempting to comply with FACTA, HIPPA, GLB etc ...

According to Betsy Broder of the FTC.. “all businesses should look to the law for guidance on how to protect consumer data. At a basic level, she says, **that means businesses need to have a plan in writing describing how customer data is to be secured and an officer on staff responsible for implementing that plan. “We will act against businesses that fail to protect their data ... all businesses must be able to show they have a written security plan in place. “We’re not looking for a perfect system .. But **we need to see that you’ve taken reasonable steps** to protect your customers’ and employees’ information”.**

Presentation Bonus

- To obtain sample forms* of:
 - Appointment of Security Compliance Officer
 - Sensitive & Non Public Information Policy
 - Mandatory Employee Meeting Notification
 - Use of Confidential Information By Employee

Hand in your business card and/or send an email containing your mailing address & phone number to:

rlisterman@btr-security.com

- * **Forms contain copyrighted material that can only be delivered after agreement to terms and conditions for their application and use. Details will be covered once contacted with the above requested information. Thank you for your attendance today, we look forward to helping you with this bonus information. There is no charge for this service.**

Law Firms Are Trolling for Victims

LIEFF CABRASER
HEIMANN & BERNSTEIN, LLP

for the plaintiffs
since 1972

OUR FIRM ATTORNEYS SUCCESSES CONTACT US SEARCH



- HOME
- OFFICES
- CURRENT CASES
- PRACTICE AREAS
- MEDIA CENTER
- ARTICLES
- NEWS
- ABOUT CLASS ACTIONS
- CLASS NOTICES
- NEWSLETTER
- PUBLIC INTEREST CASES
- RECENT TRIALS
- LEGAL LINKS
- EMPLOYMENT
- DISCLAIMER
- PRIVACY
- SITE MAP

Identity Theft Fraud Investigation and Lawsuits

Almost 20 per cent of US consumers have fallen victim to identity theft, and younger adults are at greatest risk, according to an Experian-Gallup Personal Credit Index published August 4, 2005. Roughly 25% of American consumers under 30 have had their financial information stolen, the study found.

Identity theft is rampant and the problem is growing worse -- in recent months there have been numerous reports about breaches, breaks and improper disclosures at large corporations, resulting in release of secret personal identity data and financial information. Suddenly things seem out of control: instead of losing our identities one by one, we're seeing criminals grabbing them in massive chunks -- literally millions at a time.

What Is Identity Theft?

Identity theft occurs when someone takes your personal information such as your name, Social Security number, credit card number or other identifying information, without your permission to commit fraud, theft or other crimes.

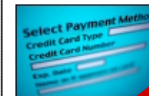
Identity theft is a very serious crime. People whose identities have been stolen can end up spending months or years -- and significant amounts of money -- cleaning up the mess thieves have made of their good name and credit record.

And despite efforts at cleanup, in the meantime victims may lose job opportunities, be refused loans, education, housing or cars, or even be arrested and incarcerated for crimes they did not commit.

www.btr-security.com

Do you suspect that a large corporation has released your private information (through an accident or otherwise)? If you are one of many thousands whose confidential information was compromised, you may have a viable class action case against that company. [Contact an attorney](#) at the national plaintiffs' law firm of Lieff Cabraser to discuss your case. Lieff Cabraser defends Americans harmed by corporate wrongdoing.

CONSUMER PROTECTION



We seek to halt unfair business practices that harm consumers nationwide. [Learn more.](#)

INJURY CASES



We represent [injured persons across America.](#)

Recent Cases:

[Ortho Evra Birth Control Patch](#)

[Guidant Heart Defibrillator Flaw](#)

[Guidant Pacemaker Warnings](#)

[Bausch & Lomb ReNu Recall](#)

Instead of losing our identities one by one, we're seeing criminals grabbing them in massive chunks -- literally millions at a time.

Do you suspect that a large corporation or your employer has released your private information (through an accident or otherwise)? If you are one of many thousands whose confidential information was compromised, **you may have a viable class action case against that company. Contact an attorney at the national plaintiffs' law firm of Lieff Cabraser to discuss your case.** Lieff Cabraser defends Americans harmed by corporate wrongdoing.

***Some companies who are currently involved in litigation
with the FTC or involved in class action law suits***

- *ChoicePoint*
- *LexisNexis*
- *DSW Shoes*
- *Equifax*
- *Veterans Administration*
- *Providence Health Systems*
- *AOL*
- *Tri-West Healthcare*
- *Ohio University*
- *BJ's Wholesale*
- *CardSystems Solutions*
- *NCsoft*
- *Bank of America*
- *SAIC*
- *Prince William County Hospital*
- *Wachovia*
- *Petco*
- *Drive Time*

*The Federal Trade Commission's recent settlement with a well known company makes an effective security program a **national requirement** for any employer that holds personal **information**, regardless of industry or specific statutory or regulatory requirements. To the FTC, a failure to develop and implement an effective information security program constitutes an **unfair trade practice**.*

“Personal Information” Defined:

- Any record about an individual, containing non-public identifying information such as SSN, DMV#, Birthdate, Financial Account #s, etc, whether in
 - paper,
 - electronic,
 - or other form such as a consumer report or is derived from a consumer report.
- Consumer information also means a compilation of such records.
- Note: Consumer information does not include information that does not identify individuals, such as aggregate information or blind data.

Disposal of Personal Information

- “For persons subject to the Gramm-Leach-Bliley Act, 15 U.S.C. 6081 et seq., and the Federal Trade Commission’s Standards for Safeguarding Customer Information, 16 CFR Part 314 (“Safeguards Rule”), incorporating the proper disposal of consumer information as required by this rule into the information security program required by the Safeguards Rule.”
- In other words: “Any person who maintains or otherwise possesses consumer information for a business purpose” is required to dispose of discarded consumer information, whether in electronic or paper form ‘by taking reasonable’ measures to protect against unauthorized access to or use of the information in connection with its disposal.”

From FTC Protecting Personal Information Guidance for Business

Safeguarding Customers' Personal Information:

- Designate the senior level employee or employees to coordinate the safeguards;
- Identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of current safeguards for controlling these risks;
- Design a safeguards program, and detail the plans to monitor it;
- Select appropriate service providers and require them (by contract) to implement the safeguards; (i.e. you are responsible for affiliates' compliance.) and
- Evaluate the program and explain adjustments in light of changes to its business arrangements or the results of its security tests.

From FTC Protecting Personal Information Guidance for Business

Take Stock: Conducting a Data Security Audit in Your Office

- Secure the scene – Take Inventory
- Look for footprints – Track personal information through your company
- Check the doors – Document how personal data enters & leaves your company
- Dust for fingerprints – Who has access to personal information (direct & indirect)
- Protect key evidence – How personal information is maintained

From FTC Protecting Personal Information Guidance for Business

Scale Down: Why Less is More When Securing Sensitive Information

- Cool, calm, and *un*collected – Stop asking for what you do not need or only when you do need it
- Don't fidget with the digits – Don't hold onto credit card information unless you absolutely need it
- Stay socially secure – Use SSN only for lawful needs
- Is your “default” at fault – Set computer defaults to be in line with your security plan
- Too much information? – Are you following current laws; at least since December 1, 2006?
- Pay attention to retention – Develop a written plan

From FTC Protecting Personal Information Guidance for Business

Lock It: Protecting Your Office from Info Thieves

- Lock, stock — or peril: Physical security including during active working hours
- Barbarians at the gate – Viruses, spyware, etc.
- We have met the enemy and he is us – Employee training in handling personal information
- Trust, but verify – You are responsible for third parties whom you share personal information; be sure to investigate their data security practices & policies.

From FTC Protecting Personal Information Guidance for Business

Pitch It: Give Personal Info the Shred Carpet Treatment

- Defeat the dumpster diver – segregate personal information for proper disposal from general trash
- Full speed a-shred – have shredders conveniently place near handlers of personal information
- Nothing to write home about – Telecommuters need to follow your procedures & policies when away from office
- Disclose how to dispose - FTC's Disposal Rule
- Is your DELETE complete? - use wipe utility programs

Thank-you for attending today; here's your presentation bonus

- **To obtain sample forms* of:**
 - **Appointment of Security Compliance Officer**
 - **Sensitive & Non Public Information Policy**
 - **Mandatory Employee Meeting Notification**
 - **Use of Confidential Information By Employee**

Hand in business card or send an email containing:

1. **mailing address &**
2. **phone number:**
rlisterman@btr-security.com

* Forms contain copyrighted material that can only be delivered after agreement to terms and conditions for their application and use. Details will be covered once contacted with the above requested information. Thank you for your attendance today, we look forward to helping you with this bonus information. There is no charge for this service.

Robert A. Listerman, CPA, CITRMS



Robert Listerman (Bob) is a licensed Certified Public Accountant, State of Michigan and has over 25 years of experience as a process improvement business consultant. He graduated from Michigan State University and became a CPA while employed at Touche Ross & Co., Detroit, now known as a member firm of Deloitte & Touche USA LLP

Bob added the Certified Identity Theft Risk Management Specialist (CITRMS) designation issued by The Institute of Fraud Risk Management in 2007. The designation is in recognition of his knowledge and experience in identity theft risk management. Over 50% of identity theft can be traced back to unlawful or mishandling of non-public data within the workplace. Recent federal and state laws have been enacted to bring both criminal and civil liability to any organization that improperly maintains data on customers, employees, vendors and even its own non-public identifying information.

Currently Bob serves his professional community as an active Board Member for the Institute of Management Accountants, Delaware Chapter. Bob serves his local community as a member of the Kennett Township, PA Planning Commission and an active member of the Kennett Rotary Club at Longwood (Gardens). Past professional and civic duties include Board of Directors for the Michigan Association of Certified Public Accountants (1997-2000) and President for the Institute of Management Accountants, Oakland County, Michigan (1994-1995).