Identity Theft

Beyond the Media
ID THEFT, THE GOVERNMENT, AND YOUR BUSINESS

Identity Theft: The Next Corporate Liability Wave Corporate Counsel, March 30, 2005

“Your phone rings. It’s Special Agent Bert Ranta. The FBI is investigating a crime ring involved in widespread identity theft. It has led to millions of dollars of credit card and loan losses for lenders, and havoc in the lives of the 10,000 victims. By identifying links between the victims, the FBI has discovered where the personal data appear to have come from: your company. The victims are some of your customers.”

The nation’s fastest growing crime, identity theft, is combining with greater corporate accumulation of personal data, increasingly vocal consumer anger and new state and federal laws to create significant new legal, financial and reputation risks for many companies.”
ID THEFT, THE GOVERNMENT, AND YOUR BUSINESS

The New Face of Identity Theft
As scams become more sophisticated, companies of all kinds find themselves at risk.

Peter Krass, CFO IT  March 15, 2005

Of all the factoids swirling around this topic, the one that may create the greatest sense of urgency is this: the Federal Trade Commission says that ID theft cost U.S. businesses and financial institutions nearly $48 billion in 2003. Nearly 13 percent of all U.S. consumers — some 9.9 million people — had their personal information misused in 2003, according to the FTC. Each ID theft costs businesses $10,200 per victim on average. And the estimated time spent resolving all these ID thefts? Nearly 300 million hours in 2003.

While most media reports of identity theft stress the consumer angle, by most accounts 50 to 70 percent of ID theft occurs in workplaces, and that figure may grow as the nature of ID theft shifts from simple rip-offs to complex efforts to defraud.
ID THEFT, THE GOVERNMENT, AND YOUR BUSINESS

Major Breaches in the News:

Jan. 22, 2007 - Chicago Board of Elections - 1.3 million voters
About 100 computer discs (CDs) with 1.3 million Chicago voters' SSNs were mistakenly distributed to aldermen and ward committeemen. CDs also contain birth dates and addresses.

Jan. 17, 2007 - TJ stores (TJX), TJMaxx, Marshalls, etc. – UNK.
The TJX Companies Inc. experienced an "unauthorized intrusion" into its computer systems. It discovered the intrusion Dec. 2006.

Dec. 5, 2006 - H&R Block – Unknown
Many past and present customers received unsolicited copies of the program TaxCut that displayed their SSN on the outside.

Nov. 15, 2006 - Internal Revenue Service - Unknown(Washington, DC) According to documents obtained under the Freedom of Information Act, 478 laptops were either lost or stolen from the IRS between 2002 and 2006. 112 of the computers held sensitive taxpayer information such as SSNs.
THE REQUIREMENTS

How Does it Happen?

- Data mishandled un-intentionally
- Dishonest Insider
- Hacker
- Spoken Word
- Transferring of NPI
- Mistaken Collection of NPI and Access
- Outside Contractors
- And many other ways
ID THEFT, THE GOVERNMENT, AND YOUR BUSINESS

Important Legislation

• FACTA
• HIPAA Security Rule
• Gramm, Leach, Bliley Safeguard Rule
• Individual State Laws - Illinois
  
  S.B. 1479, S.B. 1798, S.B. 1899, S.B. 3040
DISCLAIMER

1. 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.

2. The instructor is not an attorney, and the information provided is not to be taken as legal advice.
Fair and Accurate Credit Transactions Act (FACTA)

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

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 Individual  ($92,893 Avg.)

Be Sure To Check With Your Attorney On How This Law May Specifically Apply To You
ID THEFT, THE GOVERNMENT, AND YOUR BUSINESS

HIPPA Security Rule
April 21, 2005 - 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

Be Sure To Check With Your Attorney On How This Law May Specifically Apply To You
ID THEFT, THE GOVERNMENT, AND YOUR BUSINESS

Gramm, Leach, Bliley Safeguard Rule
Eight Federal Agencies and any State can enforce this law

Applies To Any Organization That Maintains Personal Financial Information Regarding It’s 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
THE REQUIREMENTS

Safeguard and Security Rules

Requires businesses to:

• Appoint an Information Security Officer
• Develop a written policy to protect NPI
• Hold mandatory trainings for employees
THE REQUIREMENTS

Common Myths:

- Our business keeps information secure
- We are a small business and have little NPI
- We don’t use computers
- We can design a program ourselves to meet the FTC requirements
- Our company doesn’t fall under all these laws
- We currently have a Policy in place now
TYPES OF IDENTITY THEFT

6 Forms

Financial

Criminal

Medical

DMV

Social Security

Terrorist
YOUR BEST ANSWER

IDentity Theft Loss Prevention, LLC

• Leader in the Industry
• Over 5 Years in Business
• Strategic Alliances
• Partnership Program with the FTC
• The iCAP Compliance Program
YOUR BEST ANSWER

What IDTLP does for your company

• Provide necessary documentation

• Conduct Mandatory Trainings

• Provide a “3rd Eye” Walk-through
2 Options

• Cost Program
  IDTLP provides all the materials and trainings your company needs at a 25% discount

• No Cost Program
  IDTLP provides all the materials and trainings your company needs and a voluntary protection service
No Cost Program (Most popular)

BLR says this “Provide an Affirmative Defense for the company.”

“One solution that provides an affirmative defense against potential fines, fees, and lawsuits is to offer some sort of identity theft protection as an employee benefit. An employer can choose whether or not to pay for this benefit. The key is to make the protection available, and have a mandatory employee meeting on identity theft and the protection you are making available, similar to what most employers do for health insurance … Greg Roderick, CEO of Frontier Management, says that his employees "feel like the company's valuing them more, and it's very personal."

Business and Legal Reports, January 19, 2006
The Voluntary Services ($12.95 – $35.95)

Life Events
Legal Plan
& Legal Shield

Monitoring Services

You and your identity

Restoration Services

PPLSI
THE REQUIREMENTS

ABA Journal
March 2006
THE REQUIREMENTS

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

- “Stolen Lives”, ABA Journal, March 2006
“... all business should look to that 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.**

Many large businesses entrust such planning and execution to a chief technical officer or chief privacy officer. Broder says she understands that **most small businesses cannot be expected to hire a full-time privacy specialist**, but she adds that **all businesses must be able to show they have a security plan in place.**

‘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
According to Betsy Broder of the FTC, “We will act against businesses that fail to protect their data … She understands that most small businesses cannot be expected to hire a full time privacy specialists but adds that all businesses must be able to show they have a 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’ information”.

ABA Journal, March 2006 – “Stolen Lives”

Acts as a Good Faith step in attempting to comply with FACTA, GLB, HIPAA, etc …
THE REQUIREMENTS

Corporate Board Member
July/August 2006

WHO WILL CLASS-ACTION LAWYERS GO AFTER NEXT?

On Board

In which high-risk industry is your company engaged? Nuclear power? Tobacco? How does write-downs on home loans and corporate write-downs on home loans can affect the value of your company, thus affecting the value of your shares? This is a question that many companies are asking themselves today.

In the case of the sub-prime mortgage crisis, which was caused by a combination of factors, including the lack of regulation, the overleverage in the mortgage market, and the overconfidence of investors, the consequences have been severe. Many companies have suffered significant losses, and some have even filed for bankruptcy.

A recent study by the Harvard Business School found that companies that do not have strong risk management and governance policies are more likely to be affected by lawsuits. The study also found that companies that are transparent and responsive to their stakeholders are less likely to be targeted by class-action lawyers.

In addition to the sub-prime mortgage crisis, the recent financial crisis has also highlighted the importance of strong risk management and governance policies. Companies that have strong risk management and governance policies are more likely to be able to weather the storms of the financial crisis.

A recent survey by the Corporate Governance Association found that companies with strong risk management and governance policies are more likely to be valued by investors. The survey also found that companies with strong risk management and governance policies are more likely to be able to attract and retain top talent.

In conclusion, it is clear that strong risk management and governance policies are essential for companies in today’s high-risk world. Companies that do not have strong risk management and governance policies are more likely to be affected by lawsuits and financial risks.

- A. Stanford
- Harvard University

On Board

A recent study by the Harvard Business School found that companies that do not have strong risk management and governance policies are more likely to be affected by lawsuits. The study also found that companies that are transparent and responsive to their stakeholders are less likely to be targeted by class-action lawyers.

In addition to the sub-prime mortgage crisis, the recent financial crisis has also highlighted the importance of strong risk management and governance policies. Companies that have strong risk management and governance policies are more likely to be able to weather the storms of the financial crisis.

A recent survey by the Corporate Governance Association found that companies with strong risk management and governance policies are more likely to be valued by investors. The survey also found that companies with strong risk management and governance policies are more likely to be able to attract and retain top talent.

In conclusion, it is clear that strong risk management and governance policies are essential for companies in today’s high-risk world. Companies that do not have strong risk management and governance policies are more likely to be affected by lawsuits and financial risks.

- A. Stanford
- Harvard University
Thank You!

For more information, please contact us at:

Identity Theft LOSS Prevention, LLC
7330 Turk Road
Ottawa Lake, Michigan 49267
Phone: (888) LOST MY ID