Information Security:
Gone in 60 Seconds
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.”
The Facts
The Facts

A Chronology of Data Breaches — Over 223 million data records of U.S. residents have been exposed due to security breaches since January 2005.

April 4, 2008 - University of California, Irvine (Irvine, CA) - 7,000
7,000 current or former graduate students could be at risk of identity thieves who already used stolen data to file fake tax returns for 93 students.

Mar. 28, 2008 - Antioch University (Yellow Springs, OH) – 70,000
A computer system that contained personal information on about 70,000 people was breached by an unauthorized intruder three times. The system contained the names, Social Security numbers, academic records and payroll documents for current and former students, applicants and employees.

Mar. 20, 2008 - Lasell College (Newton, MA) – 20,000
A hacker accessed data containing personal information on about current and former students, faculty, staff and alumni. Information included names and Social Security numbers.

Mar. 17, 2008 - Binghamton University (Binghamton, NY) – 300
A university employee mistakenly sent an e-mail attachment containing the names, grade point averages and Social Security numbers of junior and senior accounting students to another group of School of Management students.

ILLINOIS
Consumer Sentinel Complaint Figures
January 1 - December 31, 2007
Total Number of Fraud and Identity Theft Consumer Complaints = 31,906

Fraud Complaints from Illinois Consumers = 21,602

<table>
<thead>
<tr>
<th>Rank</th>
<th>Top Categories</th>
<th>Complaints</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Shop-at-Home/Catalog Sales</td>
<td>2,227</td>
<td>10%</td>
</tr>
<tr>
<td>2</td>
<td>Internet Services</td>
<td>1,588</td>
<td>7%</td>
</tr>
<tr>
<td>3</td>
<td>Computer Equipment and Software</td>
<td>1,173</td>
<td>5%</td>
</tr>
<tr>
<td>4</td>
<td>Foreign Money Offers</td>
<td>1,105</td>
<td>5%</td>
</tr>
<tr>
<td>5</td>
<td>Prizes/Sweepstakes and Lotteries</td>
<td>1,058</td>
<td>5%</td>
</tr>
</tbody>
</table>

1Percentages are based on the total number of fraud complaints from Illinois consumers (21,602).

Amount Paid Reported by Illinois Consumers

<table>
<thead>
<tr>
<th>Total No. of Complaints</th>
<th>Total Amount Paid/Reported</th>
<th>Total Complaints Reporting Amt Pd</th>
<th>Percentage of Complaints Reporting Amount Paid</th>
<th>Average Amount Paid</th>
</tr>
</thead>
<tbody>
<tr>
<td>21,602</td>
<td>$38,585,928</td>
<td>19,807</td>
<td>92%</td>
<td>$1,948</td>
</tr>
</tbody>
</table>

2Average amount paid is based on the total number of fraud complaints where amount paid was reported by Illinois consumers (19,807). Six consumers reported an amount paid of $1 million or more.
The Weakest Link

“From an organization’s perspective, people include employees, customers, third parties, and business partners. All of these people are vital to the organization’s survival and are privy to the organization’s information in varying degrees through different means. As a result, all of these people represent risk. Well aware that infrastructures and perimeters have been fortified, today’s sophisticated crooks no longer batter the fortress directly – they take a subtler approach through its people.”

### Definition of CSI

#### Examples of Confidential and Sensitive Information

<table>
<thead>
<tr>
<th>Personal Information</th>
<th>Business Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Social Security Number</td>
<td>Federal Identification Numbers</td>
</tr>
<tr>
<td>Social Insurance Number</td>
<td>Proprietary Information</td>
</tr>
<tr>
<td>Birth Dates</td>
<td>Trade secrets</td>
</tr>
<tr>
<td>Driver’s License Number</td>
<td>Business Systems</td>
</tr>
<tr>
<td>Professional License Information</td>
<td>Pay Rates / Payroll</td>
</tr>
<tr>
<td>Customer Identifiers*</td>
<td>Access Codes / Passwords*</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Financial Information</th>
<th>Medical Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credit Card Number</td>
<td>Medical Records</td>
</tr>
<tr>
<td>Card Expiration Dates</td>
<td>Doctor’s Names and Claims</td>
</tr>
<tr>
<td>Card CCV Numbers</td>
<td>Life, Health, Disability Insurance</td>
</tr>
<tr>
<td>Account Numbers</td>
<td>Policy Information</td>
</tr>
<tr>
<td>Credit Reports</td>
<td></td>
</tr>
<tr>
<td>Billing Information*</td>
<td></td>
</tr>
</tbody>
</table>

* This Information may not always be classified as Sensitive Data but can be used for Social Engineering by a thief. It should still be secured.
Common Causes of Information Loss or Breach

**Internal Threats**
- Poorly trained personnel
- Inadequate security measures
- Insufficient support from management
- Unsupervised third party providers
- Dishonest insiders
- Inadequate IT systems

**External Threats**
- Hackers
- Organized Crime
- Social Engineers
- Customers
- Competitors
The Facts

Six Common Forms of Identity Theft

Financial

Criminal

Medical

DMV

Social Security

Terrorist
Legislation, Loss, and Social Responsibility
Three Reasons Why Businesses Need to Safeguard Confidential and Sensitive Information.

1. Current State and Federal Legislation Requirements

2. To Limit Financial Loss and Loss of Trust

3. Social Responsibility
Important Federal Legislation

• Identity Theft Assumption and Deterrence Act

• Family Education Rights and Privacy Act

• Health Insurance Portability and Accountability Act (HIPAA): Security Rule

• Gramm-Leach-Bliley Act: Safeguard Rule

• Fair and Accurate Credit Transactions Act (FACTA)
  • Identity Theft Red Flags Rule (Sections 114 and 315)

• Social Security Number Privacy Act
State Legislation

Common Law

“As a fundamental principle, even before reaching theories applicable to information security, parties are generally responsible under the common law of torts to use due care in handling the information regarding others.” 2 Businesses that do not take reasonable steps to protect information could be held civilly liable for criminal acts committed by others with the stolen information. This was the outcome of Bell v. Michigan Council 25 of the AFSCME, 2005 Mich. App. LEXUS 353(Mich. Ct. App. Feb. 15, 5005).

State Identity Theft Notification Laws

To date, 39 states have victim notification laws in place. In Illinois, a business must notify potential victims within a reasonable period of time.
Financial Loss and Loss of Trust

If confidential and sensitive information is lost or stolen damages go beyond government fines, penalties, and potential imprisonment.

Perhaps the greatest impact to business is negative publicity and loss of trust among consumers.

“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!”

Calculate the Cost of a Breach

By taking the time to properly prepare your business, you may calculate your savings with the following formula:

**Business Assets**

+ Revenue
- Liabilities
- Expenses
- Class Action Lawsuits
- Notification fines
- Monitoring Services
- Crisis Management
- Forensics
- Federal and State Fines (depending on the law)
- Attorney Fees
- Bad Publicity
- Jail Time

= Potential Loss
Social Responsibility

Any organization that collects and / or retains personal, financial, medical, and business information has an ethical and a social responsibility to safeguard that information.
Workplace Requirements
Workplace Requirements

Compliance Standards for the Protection of Confidential and Sensitive Information

There can be “safe harbor” for businesses that make a reasonable effort to safeguard confidential and sensitive information. This includes:

1. The designation of an Information Security Officer.

2. A risk assessment of material internal and external risks to the security of confidential and sensitive information.

3. The design and implementation of a written Information Security Policy.

4. Employees must be trained on security policies.

5. The evaluation and adjustment of the program in light of the results of testing and ongoing monitoring of the program.

6. A plan for security incidents.
The *information* Compliance and Awareness Process
The Eight Stage - *information* Compliance and Awareness Process

**Stage One:** Investigate Identity Theft, Fraud, and Information Security Risks

**Stage Two:** Designate an Information Security Officer

**Stage Three:** Define CSI and Information Systems

**Stage Four:** Take Inventory of Information Assets

**Stage Five:** Assess Risks to Information Systems

**Stage Six:** Design an Information Security Policy

**Stage Seven:** Implement Security Measures

**Stage Eight:** Monitor and Evaluate Security Program
Disclaimer

This information Compliance and Awareness Program (iCAP) does not guarantee compliance with any Federal or State Government requirements. There is no guarantee against security incidents. This program is intended to help businesses to make a reasonable effort to reduce the likelihood of identity theft and fraud.
Safeguarding personal, business, financial, medical information is everyone’s responsibility! We are here to help.

Identity Theft LOSS Prevention, LLC

7330 Turk Road

Ottawa Lake, Michigan 49267

888 – LOST MY ID

www.idtlp.com