Affirmative Defense Response System℠

Why should all businesses, corporations, schools, financial institutions and hospitals be concerned about Identity Theft, FACTA, HIPAA, and GLB?

Answer: Liability, both civil and criminal.

Five Common Types of Identity Theft

Drivers License

Social Security

Medical

Character/ Criminal

Financial

Identity Theft is not just about Credit Cards!

ID Theft is an international crime and access to an attorney may be critical

What is Identity Theft?

Why You Are At Risk

Social Security Number
SSA DBS

Insurance Claims
C.L.U.E. DBS, etc

Your Name
1000's of aggregators

Address
1000's of DBS

Driver's License # & Record
DMV DBS

Fingerprints and DNA
FBI, State, and Local DBS

Military Record
DOD DBS

Legal History
State and Federal Court DBS

Criminal History
NCIC DBS

Credit History
Credit Repositories' DBS

Real Estate Deeds
Clerks of Court DBS

Birth Certificate
Choice Point DBS, State, etc

Car Registration & Info
DMV, Local Treasurer, On Star, etc

Medical Records
MIB DBS, etc

Phone Number and Tracking Info
1000's of aggregators

The Databased You

Take Charge: Fighting Back Against Identity Theft

Order the Federal Trade Commission's free report!

Phone: 877.IDTHEFT
Web: **http://www.consumer.gov/idtheft**

When you read this, it will become crystal clear why it is good for the company and the employee to have an ID Theft service that offers legal access, monitoring, and restoration versus resolution or reimbursement.

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 15th, 2006

Important Legislation

- **FACTA**
- **HIPAA Security Rule**
- **Gramm, Leach, Bliley Safeguard Rule**
- **Individual State Laws (i.e. Texas Whistle Blower Statute)**

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

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

HIPAA 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

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

Gramm, Leach, Bliley
Safeguard Rule

Any Organization Includes:

- Financial Institutions*
- Schools
- 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.

Safeguard and Security Rules

Requires businesses to:

- Appoint an Information Security Officer
- Develop a written policy to protect NPI
- Hold mandatory trainings for employees who have access to NPI

Appointment of Security Compliance Officer

August 1, 2006

[insert employee designee]

RE: Appointment of Security Compliance Officer

Dear [employee]:

As part of [Company's] comprehensive information security program, we are pleased to appoint you as Security Officer. As Security Officer you will be responsible to design, implement and monitor a security program to protect the security, confidentiality and integrity of personal information collected from and about our employees, consumers and vendors.

As Security Officer you will help [Company] identify material internal and external risks to the security of personal information; design and implement reasonable safeguards to control the risks identified in the risk assessment; evaluate and adjust the program in light of testing results; and continuous monitoring of the program and procedures.

As Security Officer, [Company] will provide you access to training courses and materials on a continuing basis.

Thank you for your commitment to [Company].

Sincerely,

[Company]

Chief Executive Officer

Sensitive and Non Public Information Policy (First of four pages)

SENSITIVE and NON PUBLIC INFORMATION POLICY

1. PURPOSE

The company adopts this policy to help protect employees, customers, contractors and the company from damages related to loss or misuse of sensitive information. This policy will:

- Define sensitive information
- Describe the physical security of data when it is printed on paper
- Describe the electronic security of data when stored and distributed

2. SCOPE

This policy applies to employees, contractors, consultants, temporaries, and other workers at the company, including all personnel affiliated with third parties.

3. POLICY

3.1. Definition of Sensitive Information

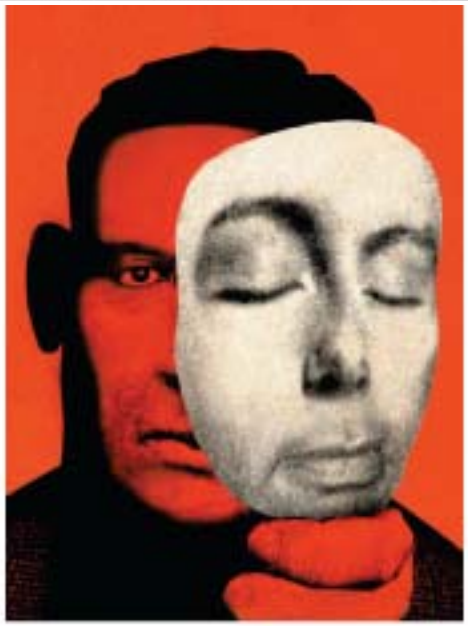
Sensitive information includes the following items whether stored in electronic or printed format:

3.1.1. Personal Information - Sensitive information consists of personal information including, but not limited to:

3.1.1.1. Credit Card Information, including any of the following:

- Credit Card Number (in part or whole)
- Credit Card Expiration Date
- Cardholder Name
- Cardholder Address

ABA Journal
March 2006



Victims of Identity Theft Start Looking for Damages From Companies That Held Their Personal Financial Information

JASON KRAUSE

STOLEN LIVES

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**.

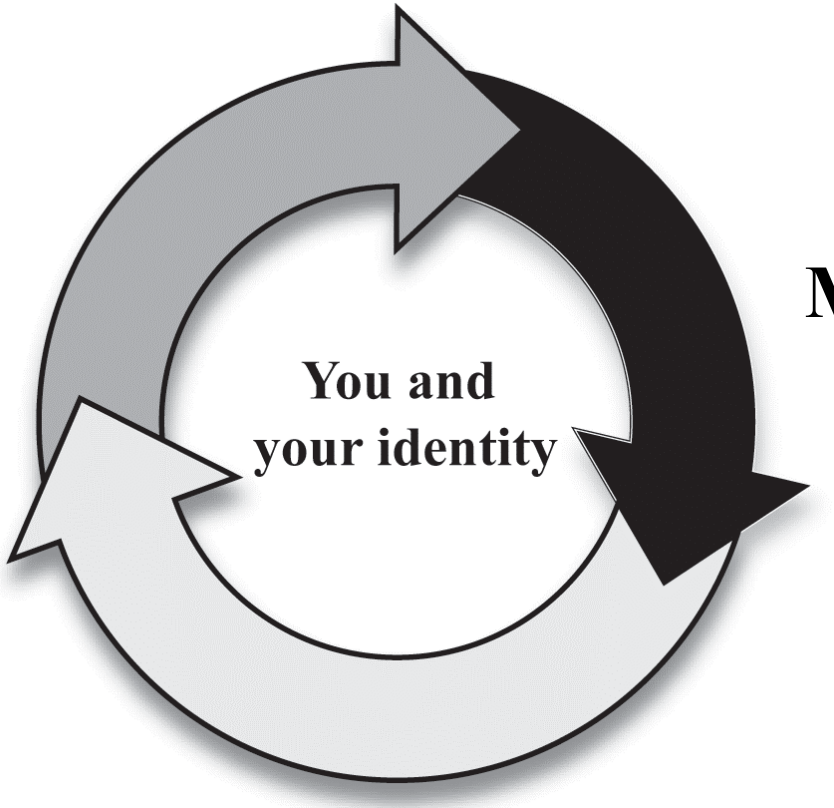
Many large businesses entrust such planning and execution to a chief technical officer or chief privacy officer. Broder says she understands that **most small businesses cannot be expected to hire a full-time privacy specialist,** but she adds that **all businesses must be able to show they have a security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

The Best Answer …

Life Events
Legal Plan
&
Legal Shield



Monitoring Services

Restoration Services

The Best Answer

Pre-Paid Legal Services, Inc. is the only company with a suite of services: Life Events Legal Plan, Legal Shield and the Identity Theft Shield which provide help in every phase of *Identity Theft* – before, during, and after the crime occurs. The Affirmative Defense Response System^{SM} was developed to provide businesses and their employees a way to minimize their risk in regard to Identity Theft.

Why and How We Help You…

1. First Reasonable Step To Protect Customer's Information As Outlined By The FTC

To All Employees
[Company]

RE: MANDATORY EMPLOYEE MEETING
PRIVACY AND SECURITY COMPLIANCE PROGRAM AND IDENTITY THEFT TRAINING
[insert date, time and location]

On [insert date], [company] will host a mandatory employee meeting and training session on identity theft and privacy compliance. Additionally, as an employee, you will be provided an opportunity to purchase an identity theft product.

As you know, [company] makes every effort to comply with all Federal Trade Commission guidelines to protect personal employee, customer and vendor information. As part of our security program, we want to train all employees on concrete steps to help reduce the risk of security breaches and identity theft.

This program is important to [company] and your attendance is mandatory. I look forward to seeing each of you there on [date].

Sincerely,
[Company] CEO

* Subject To Terms And Conditions

Why and How We Help You…

2. May Reduce Company Losses

The plan has Full Restoration*, which means the majority of the time in restoring an employee's identity is covered by the membership and not done on company time and/or company expense. Also, use of our Life Events Legal Plan provides help* that address related issues.

* Subject To Terms And Conditions

Why and How We Help You…

3. Potential Early Warning System

If a number of your employees get notified of improper usage of their identities, this may act as an early warning system to your company of a possible internal breach.

Why and How We Help You…

4. **BLR says this "Provides 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

Identity Theft Protection and Legal Services

As an employee of _____, located in _____, I acknowledge that a Pre-Paid Legal Services, Inc., independent sales associate made available to me the Identity Theft Shield and a Pre-Paid Legal Services, Inc. membership.

- Identity Theft Shield:
  - Initial credit report and guide on how to read the report
  - Continuous credit monitoring
  - Identity restoration in the event of a theft

- Pre-Paid Legal Services Plan:
  - Preventive legal services provided through a network of independent provider attorney law firms in each state and province
  - Phone Consultation with Attorneys/Review of Documents/Phone Calls and Letters for any legal matter and issues regarding identity theft including concerns regarding my: 1) drivers license, 2) medical information, 3) social security number, 4) character/criminal identity, and 5) my credit identity and information
  - A Will for me and my spouse
  - Motor vehicle moving violation representation
  - Trial defense
  - IRS audit
  - Legal Shield 24 hours a day, 7 days a week when arrested or detained
  - Discounted rate for other legal services

I have seen and read the brochures listing the specific benefits, limitations and exclusions of these plans. The company made these benefits available to me at my expense.

___ I have decided to enroll in both plans.

___ I have decided to enroll in the legal plan only.

___ I have decided to enroll in the Identity Theft Shield only.

___ I have decided not to enroll in either plan.

Name: _____ Date:_____

Signature: _____ Witness:_____

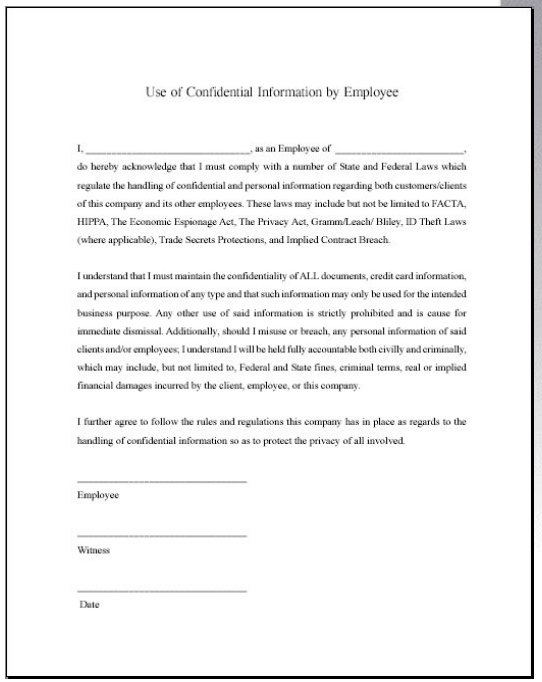
Why and How We Help You…

5. Mitigating Damages

To potentially protect yourself, you could have all employees sign this document…

- It makes Employees **aware** of their legal responsibilities to protect NPI
- It serves as **proof** that handlers of NPI have been through the mandatory training required by law

Use of Confidential Information by Employee



Use of Confidential Information by Employee

I, _____, as an Employee of _____, do hereby acknowledge that I must comply with a number of State and Federal Laws which regulate the handling of confidential and personal information regarding both customers/clients of this company and its other employees. These laws may include but not be limited to FACTA, HIPPA, The Economic Espionage Act, The Privacy Act, Gramm/Leach/ Bliley, ID Theft Laws (where applicable), Trade Secrets Protections, and Implied Contract Breach.

I understand that I must maintain the confidentiality of ALL documents, credit card information, and personal information of any type and that such information may only be used for the intended business purpose. Any other use of said information is strictly prohibited and is cause for immediate dismissal. Additionally, should I misuse or breach, any personal information of said clients and/or employees; I understand I will be held fully accountable both civilly and criminally, which may include, but not limited to, Federal and State fines, criminal terms, real or implied financial damages incurred by the client, employee, or this company.

I further agree to follow the rules and regulations this company has in place as regards to the handling of confidential information so as to protect the privacy of all involved.

_____
Employee

_____
Witness

_____
Date

Be Sure To Check With Your Attorney Before Using A Form Such As This

Use of Confidential Information by Employee of ABC Corporation

I, _____, as an employee of _____, do hereby acknowledge that I am subject to and must comply with a number of State and Federal laws involving the confidential handling of personal information regarding both customers/clients of ABC Company and other employees. These laws may include but not be limited to FACTA, HIPPA, The Economic Espionage Act, The Privacy Act, Gramm/Leach/Bliley, Identity Theft laws [where applicable], Trade Secrets Protections, and Implied Contract Beach.

I acknowledge that I must maintain the confidentiality of all documents, credit cards, and personal information of any type and that such information may only be used for their intended business purpose. Any other use of said information is strictly prohibited and is cause for immediate dismissal. Additionally, should any misuse of information be made by me I understand that I am fully accountable both civilly and criminally.

I further agree to follow the rules and regulations of ABC Company in regard to the handling of confidential information so as to protect the privacy of all involved.

_____ _____

Employee Date

_____

Witness

Employee Confidentiality Document

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

ABA Journal, March 2006 – "Stolen Lives"

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".**

Employers Offer Help Fighting ID Theft

Wall Street Journal, May 24, 2006

"As Identity Theft continues to claim millions of victims, a growing number of employers are offering to help affected workers pick up the pieces.

Companies including drugstore chain **Rite Aid Corp.**, publisher **Reed Elsevier PLC**, and **Quest Communications International Inc.** **have recently been signing up for identity-theft resolution services to offer their employees as a workplace benefit**. The companies say **the service can reduce the time employees spend during work hours filing reports and talking with creditors to resolve the problems created by identity theft**. Providers of the services say they help victims clear their name, restore their credit and prevent future problems.

A recent survey of human-resources managers conducted by Aon Consulting, a unit of Aon Corp., found that 2% of employers currently offer identity-theft services as a workplace benefit, and a further 4.6% said they expected to offer it in the near future. Security and insurance experts say the **interest also stems from concern among employers that they might face liability for personal data they have put at risk. By offering employees recovery assistance, companies hope to head off possible lawsuits**, these experts say.

The heightened attention comes as disclosures of personal-date security breaches, which can lead to the crime of identity theft have soared. This week, the Department of Veterans Affairs said personal data - - including Social Security numbers - - on 26.5 million veterans and some of their spouses were stolen this month, although there isn't any evidence they have yet become victims of financial fraud. The lapse brings to more than 80 million the number of identities since early 2005 that have been put at risk through such data breaches, according to Privacy Rights Clearinghouse, a non-profit advocacy group."

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.

Your mind begins to whirr. Are there other customers affected who haven't been identified yet? Is it a hacker or an inside job? **Is your company also a victim here, or could it be on the wrong end of a class action lawsuit?**

You recall reading that each identity theft victim will on average spend $1,495, excluding attorney's fees, and 600 hours of their time to straighten out the mess, typically over the course of a couple of years. For out-of-pocket costs alone that is, say, $2,000 per victim. Multiplying that by 10,000 customer victims equals $20 million. Adding as little as $15 per hour for the victims' time and you get $11,000 per case or a total of $110 million in total even before fines and punitive damages are considered. And that's on top of the potential impact on your company's future sales.

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."

Health System Faces Class Action Lawsuit After Records Theft

iHealthbeat.org, February 1, 2006

"**A former patient of Providence Health System on Monday filed a class action suit against Providence on behalf of the 365,000 people whose records were stolen from an employee's car**, the *Oregonian* reports. The theft has 'triggered state and federal inquiries and revived efforts to enforce stronger privacy protections,' according to the *Oregonian*.

The lawsuit, which is the first to be filed in connection with the theft, **seeks an immediate court order requiring the not-for-profit Providence to arrange and finance ongoing credit monitoring for individuals whose records were stolen and to pay for any damaged credit ratings**.

Providence on Jan. 25 began notifying patients of the Dec. 31 theft. Providence's home services division designated certain employees to take home the unencrypted computer files each day as an emergency backup, according to Rick Cagen, chief executive of Providence's Oregon operations. Providence now uses encryption to protect backup files and sends them to a secure off-site facility.

Providence said it would help anyone whose credit is harmed by the theft, and Cagen said the organization would decide what kind of help to provide on a case-by-base basis, the *Oregonian* reports.

'I don't think that's enough,' said David Sugerman, an attorney representing the former patient who filed the suit. He said he has received reports from two people whose records were stolen, who say that they have had their identities stolen. Sugerman said Providence has an obligation to set up and finance efforts to prevent identity theft instead of leaving it up to individuals, the *Oregonian* reports (Rojas-Burke, *Oregonian*, 2/1)."

Corporate Board Member July/August 2006

WHO WILL CLASS-ACTION LAWYERS GO AFTER NEXT?

In which high-risk industry is your company engaged? Nuclear power? Tobacco? How about soft drinks or home loans? Corporate attorneys say cola makers and mortgage lenders could both be popular targets of the plaintiffs' bar in the years ahead.

True, your odds of being hit with a class-action lawsuit fell a bit last year; there were only 2.4 such filings for every 100 publicly traded U.S. companies, down from 2.8 in 2004. But plaintiffs' attorneys have hardly gone on holiday, and they've shown a nimble ability to home in on fresh prey when traditional targets begin to yield fewer pickings. According to Stanford Law School's Securities Class Action Clearinghouse, filings against companies in two of the most-sued industries of 2004, technology and communications, were down 32% last year. But filings against consumer companies increased, rising 11% for noncyclicals, such as food and beverage outfits, and 38% for cyclicals, such as automakers, airlines, and leisure businesses.

Which companies are likely to find themselves in the hot seat in the years ahead? Attorneys speculate that they will include:

FAST-FOOD AND SOFT-DRINK MANUFACTURERS. Thirty years after they took on the tobacco industry, plaintiffs' attorneys are zeroing in on companies whose products might be linked to obesity. Never mind that most suits of this kind have thus far gone nowhere; the three-decades-long battle against tobacco, which produced a $246 billion settlement in 1998, shows that the plaintiffs' bar has plenty of patience. The Center for Science in the Public Interest has already announced that it will sue food manufacturer Kellogg Co. and Viacom Inc., owner of CBS, MTV, and Nickelodeon, to stop them from marketing foods high in sugar, saturated fat, trans fat, or salt to children. The center also has plans to sue Coca-Cola, PepsiCo, and other companies to get soft drinks out of public schools. Meanwhile, McDonald's is still wrestling with a class-action lawsuit filed in 2002—initially dismissed but reinstated last year—on behalf of two New York City teenagers who claim that its Big Macs and Happy Meals made them McFat.

MAKERS OF PHARMACEUTICALS AND MEDICAL DEVICES, AND HEALTH-CARE PROVIDERS. Companies that push the boundaries of science in an effort to change the way the human body performs have always been engaged in risky business. And the aging of the baby boomers—the 76 million people born between 1946 and 1964—presents a whole new wave of customers for them to target. "Plaintiffs' lawyers go where the food is," says the general counsel of a NASDAQ-listed company in an unrelated industry, who asks to be anonymous. "If there's any sort of junk science out there that suggests a medical device or drug is in any way linked to hiccups, it's going to trigger a class-action lawsuit." Michael J. Mueller, a partner, litigator, and leader of the class-action team at Akin Gump Strauss Hauer & Feld in Washington, D.C., suggests that as employers push employees into so-called consumer-driven health-care plans, in which the employees pay for more services directly, health-care providers could be hit with class-action suits over billing practices if patients conclude that they have been improperly charged. The baby boomers' aging, warns Mueller, might also prompt more lawsuits in areas such as nursing-home abuse, retirement-fund fraud, and disability discrimination.

CHRIS GAK

ON BOARD

FINANCIAL INSTITUTIONS. With interest rates rising, some attorneys warn that mortgage lenders and credit-card companies may find themselves under attack from variable-rate borrowers who are suddenly unable to meet their monthly payments. The likely argument from the plaintiffs: Overzealous lenders allowed them to borrow more than they could afford to repay, charged illegal fees, or otherwise mismanaged their accounts. There's precedent for such actions. Early this year Ameriquest Mortgage Co., which specializes in making home loans to borrowers with poor credit, agreed to a $325 million settlement of a suit alleging that it had defrauded and misled customers.

CONSUMER-PRODUCTS COMPANIES AND GOVERNMENT-REGULATED COMPANIES. Attorneys say directors should pay special attention to litigation threats at companies where products are recalled for safety reasons and at government-regulated outfits that become the subject of investigations, hearings, or findings by governmental bodies.

COMPANIES WITH ACCESS TO SENSITIVE DATA ABOUT CUSTOMERS AND EMPLOYEES. Yes, this applies to just about everybody, but with concerns about identity theft zooming, any company that accidentally discloses data protected by privacy laws runs a risk of litigation. BJ's Wholesale Club is being sued, for example, by an organization of credit unions called CUNA Mutual over allegations that BJ's failed to protect the credit-card information of its customers. The retailer entered into a settlement with the Federal Trade Commission last year in the matter, agreeing as part of the deal to beef up its data-security processes. Although these cases don't appear to have prompted any litigation yet, several big companies suffered high-profile losses of sensitive data last year, including Citigroup Inc.'s CitiFinancial unit, Bank of America, and Time Warner. The two financial institutions reported that computer tapes containing sensitive information about customers, such as their Social Security numbers, were lost while being moved to offsite locations by delivery companies. Similar Time Warner computer tapes went missing during transport to a backup facility by a records-management company. All three corporations said there had been no reports that the compromised information had been misused.

If you're on the board of a company that finds itself under the gun in any of these areas, Sheila L. Birnbaum has some advice. Birnbaum is the partner who heads the complex mass-tort and insurance group at the New York City headquarters of Skadden Arps Slate Meagher & Flom. She says the board must be open about any missteps the company might have made and must avoid doing anything that suggests a cover-up. Akin Gump's Michael Mueller advises directors of any company operating in a high-risk industry to cultivate a culture of compliance and insist that legal counsel vet all advertising, product labeling, product literature, and other public statements that might be relied upon by people using the product. He also says such companies should select their business partners carefully. "Vendors and suppliers should be able to indemnify manufacturers," he says, "while downstream sellers should inquire from upstream suppliers as to their quality-assurance programs and remedies for defective products."

DIRECTORS OF ANY COMPANY IN A HIGH-RISK INDUSTRY SHOULD INSIST THAT LEGAL COUNSEL VET ALL ADVERTISING, PRODUCT LABELING, AND PRODUCT LITERATURE.

Even if a company isn't on this list of potential class-action targets, legal experts recommend that boards take measures to head off trouble and anticipate problems. Directors should make sure their companies pay attention to hot-button accounting issues such as revenue recognition, channel stuffing, and classification of expenses. They should be alert to any spike in negative media coverage related to their company or industry, and to complaints made to government regulators. And they should advise management to assign in-house or outside counsel to monitor the Internet periodically for warning signs of class-action litigation. Good places to look include websites operated by plaintiffs' law firms and various clearinghouses for class actions. Among the latter are Stanford's Securities Class Action Clearinghouse (www.securities.stanford.edu) and Lawyers and Settlements (www.lawyersandsettlements.com), a site run by Online Legal Marketing Ltd. that lists new lawsuits and settlements and solicits plaintiffs. Companies should also monitor financial chat rooms and product-review sites; plaintiffs' lawyers sometimes use them to build cases and locate clients and witnesses.

In today's litigious climate, no board or company is immune to the threat of a lawsuit. There's no reason to be blindsided.

by Randy Myers

CORPORATE BOARD MEMBER/SPECIAL ISSUE: LAWYERS JULY/AUGUST 2006

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.

1. Get a firm understanding of the Important Legislation we talked about today.

- A great site with a tremendous amount of information is the FTC PUBS index: http://www.ftc.gov/bcp/conline/pubs/
- FACTA: www.ftc.gov/os/2004/11/041118disposalfrn.pdf
- HIPAA: www.hipaa.org
- Gramm-Leach-Bliley Act: www.ftc.gov/os/2002/05/67fr36585.pdf
- Two great resources for white papers: www.omnirim.com www.recall.com

2. Take the first reasonable step as outlined by the FTC and schedule mandatory meetings regarding identity theft for your employees

3. Based on provisions in HIPAA and Gramm-Leach-Bliley, appoint an Information Security Officer.

4. Make sure "Good Faith" measures are in process. Confirm in writing, keep and put in employee file for your protection.

5. Review Employee Confidentiality Form and everything else you have questions on with your counsel.

6. You may want to review the recent publication from the Better Business Bureau: **www.bbb.org/securityandprivacy/download.asp**

7. When would you like us to begin working with your staff and/or employees?