



# Direct Defender Presents Private Information Compliance

***"The majority of data breaches are caused by insiders."***

Sensitive information leaves the company every day through portable devices, emails and laptops. Trained employees equipped with proven security policies and strategies ensure your compliance with privacy legislation and plug the biggest information security threat your company faces.

## Who Needs A Privacy Compliance Program?

- ❖ Your company retains customer information or personally identifiable information (PII) that might be a target for Identity Theft.
- ❖ Your company maintains sensitive information, customer data or trade secrets.
- ❖ Legislation requires you to train new employees on the threats and vulnerabilities of company computing systems and personal information.

**“Noncompliance could cost you or your business up to \$1,000,000 in fines and up to 10 years in prison per incident!”**

Numerous regulations (primarily federal, but also global and state) have been enacted to defend those affected by a personal information security breaches.

They each address the common failure points and the possible negative consequences of private information breaches.

Most companies are aware of the **Sarbanes-Oxley Act, SEC 17a-4**, and the Statement on Auditing Standards. Customer-oriented organizations know about **Gramm-Leach-Bliley**. Those working in healthcare adhere to **HIPAA**. The financial services sector complies with the **Payment Card Industry Data Security**.

Most industries are subject to very particular laws in respect to personal data protection. All organizations must implement and demonstrate every effort to prevent a data-at-rest information security breach.

No matter what type of business or industry, data that is meant to be maintained as private must not be allowed go public due to an obvious neglect. Failure to pre-empt or implement compliance policies could allow a breach to completely destroy a business.

Because a personal information breach can involve tens of thousands of identities, the costs and fines involved are often millions of dollars.

### Who Is At Risk?

Any company with responsibility for storing the personal data of customers and employees may be at risk.

Businesses must anticipate legal liability for identity theft incidents and data breaches of their systems. Most liability insurance products for business exclude damages resulting from identity theft.

Your affirmative defense solution must be strong enough to defend you in a lawsuit; showing written proof of your due diligence to comply with the laws.

On May 3, 2007, lawmakers began the process of passing the overarching **Personal Data Privacy & Security Act and the Notification of Risk to Personal Data Act** (which were passed by Senate committee and introduced into the full Senate).

This legislation is meant to be a double-fisted punch in the fight against identity theft. This legislation specifies directives and increases personal liability associated with breaches to the protection of individually identifying data.

**“Both those failing to protect personal information and any party or parties benefiting from that failure can be prosecuted.”**

More than 38 states require notification when a security breach presents a reasonable risk of identity theft. No industry or particular size of company is exempt and the security breach laws may vary by state.

Violations of the federal laws include **staggering federal and state fines as high as \$1 million per occurrence**, civil liability for victim losses (including class actions), and in some instances the legislation provides for **removal and imprisonment** of culpable business executives and employees responsible for the data loss.

### Common Causes of Data Loss:

- ✓ **Negligent Employees**
- ✓ **Insiders not authorized for database use.**
- ✓ **Compromised PCs (with Trojans/backdoors).**
- ✓ **Disgruntled Insiders With Authorized Access**
- ✓ **Loss of Laptops or Flash Drives**
- ✓ **Vulnerable Web Servers or Extranets**

# Privacy Compliance Solutions

## What Can Direct Defender Do For My Company?

A step by step Affirmative Identity Theft Prevention & Privacy Governance program

Identity Fraud Monitoring of all employees

Complete Identity Theft Recovery Plan

Data Breach Action Plan and notification of victims and agencies concerned

OECD Fair Information Principles, including an easy to follow Privacy Assessment

A step-by-step checklist to easily implement a preemptive privacy governance program

Security Training Presentation for Your Employees & Custom Training Handouts

A fully managed method of dealing with Identity Theft.

Direct Defender actually repairs the damage and restores the victim's good name and credit to its pre-Identity Theft state.



Our real-time identity monitoring and our unprecedented identity-recovery success rate have made us the favorite identity theft solution across the nation.



**Direct Defender's** technology provides affordable and effective protection to companies in the event of a corporate data breach. **This program protects the covered company and its customers, alerting affected customers in the event of a breach, providing a single site 800 number for breached customers to contact, assisting the company in required agency notifications, and recovering any resulting Identity Theft.**

**Direct Defender**  
Identity Solutions

800-797-5753



[WWW.DIRECTDEFENDER.BIZ](http://WWW.DIRECTDEFENDER.BIZ)