

# Privacy Breaches: Protecting Your Business in Today's Legal Landscape

**PortAuthority Technologies, Inc.**

Three Palo Alto Square  
3000 El Camino Real, Suite 100  
Palo Alto, California 94306-2122  
Tel 650-739-0991  
Fax 650.739.0992  
[www.portauthoritytech.com](http://www.portauthoritytech.com)  
[info@portauthoritytech.com](mailto:info@portauthoritytech.com)

## Table of Contents

<b>Introduction:</b>	
<b>Protecting Corporate Data is Not Just for Good Measure—It's the Law.....</b>	<b>3</b>
<b>The New Legal Landscape for Information Security.....</b>	<b>4</b>
<b>A Growing Legal Responsibility.....</b>	<b>6</b>
<b>Calculating the Costs.....</b>	<b>7</b>
<b>Applying the DRIP Approach.....</b>	<b>8</b>
<b>PortAuthority Protects Against Information Leaks.....</b>	<b>10</b>
<b>Contributing Author: Gerard M. Stegmaier, Esq. ....</b>	<b>11</b>
<b>Sponsored by PortAuthority Technologies™ .....</b>	<b>11</b>

**Personal Information** refers to information about a person that identifies or describes an individual, it can include, but is not limited to, name, Social Security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. This piece or these pieces of information readily identifies the specific individual.

## Introduction: Protecting Corporate Data is Not Just for Good Measure—It's the Law

Guarding customer, employee, and proprietary corporate information has always been a priority for companies, but recent developments on the legal, regulatory, and legislative fronts are turning the protection of data privacy from best practices into de facto legal requirements. Law professionals, who previously encouraged their clients to institute solid information security practices as a good way to earn their customers' trust and protect their employees, now advise clients that they may be held accountable for information misuse when data confidentiality is compromised. Companies must be aware that there could be serious consequences for those that do not follow this advice.

A number of cases in the last two years demonstrate a legislative and regulatory trend to hold companies responsible for security breaches that involve the leaking of customer data. Businesses from Barnes & Noble to Time Warner have come under fire for failing to adequately protect consumer information.

## The New Legal Landscape for Information Security

The regulatory landscape is changing. In the past, the Federal Trade Commission (FTC) prosecuted companies who made unfair and deceptive statements in their marketing with regard to information security. In other words, the FTC pursued companies who promised to secure the personal information of their customers and then failed to do so. Companies such as Petco, Tower Records, and Barnes & Noble all found themselves subject to FTC scrutiny in 2005 because they made promises to guard consumer data and then didn't live up to those promises.

Businesses may have information security obligations regardless of whether they have expressly made any information security promises. Recent regulatory activity and litigation by state attorney generals, suggests that any organization collecting consumer data may have an obligation to protect that data even if it does not explicitly make such a promise. Thus, by virtue of receiving consumer information, an organization may have an obligation to protect it.

A specific example of the risk of failing to adequately secure customer information occurred at BJ's Wholesale Club. Consumer credit card numbers were stolen from BJ shoppers through BJ's Wholesale Clubs computer networks. The stolen credit card numbers caused considerable financial damage to their rightful owners.

As a result, BJ's Wholesale Club, Inc. agreed to settle charges brought by the FTC for its failure to take reasonable and appropriate measures to secure the personal information of customer data collected at its stores. According to the FTC, this information was used by an unauthorized person or persons to make millions of dollars of fraudulent purchases. The settlement requires BJ's to implement a comprehensive information security program and obtain audits by an independent third-party security professional every other year for 20 years.

Just a few years ago, specific legal requirements for privacy and information security in the United States were found primarily in specialized regulated industries such as health care, finance, and telecommunications. The experience from those industries is creating pressure for new laws and new accountability across all industries. Thus, as the example of BJ's Wholesale Club demonstrates, the burden of responsibility for the protection of private information is now placed on the organization collecting the information. This establishes de facto legal requirements for retailers and other businesses similar to the legal requirements of the health care, finance, and telecommunications industries.

Another widely publicized breach of data privacy occurred in June, 2005, when CardSystems Solutions, a credit-card processing company, failed to protect the personal information of 40 million customers. In testimony to the United States Congress, senior executives from Card Systems said the company was on the brink of shutting down because of the security failure's impact.

Federal laws, including Sarbanes-Oxley, HIPAA, the Gramm-Leach-Bliley Act (GLBA), and the Computer Fraud and Abuse Act of 1984, are having a significant impact on how companies protect private customer and employee information. For example, the agencies which implement the GLBA recently issued guidance suggesting that financial institutions may have to perform an assessment of their vendors, which could include an audit to ensure their service providers have adequate security. Previously, most financial institutions operated under the view that the presence of strict confidentiality agreements with vendors was an adequate means of addressing information security concerns.

At the state level, nearly all states have now introduced legislation designed to protect and secure personal information consumers provide to businesses. California, in particular, has been a model and key battleground. For example, California has enacted a statute requiring companies to notify consumers whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. CAL. CIV. CODE § 1798.82 (2005).

## A Growing Legal Responsibility

The current legal and regulatory landscape has a great impact on corporate data security responsibilities. Organizations are clearly being held to a higher standard with regard to information security. Attorney Generals in a number of states are holding businesses directly responsible for these breaches, as evidenced through their vigorous prosecutions. The Attorney General of Ohio, discussing the state's prosecution of shoe discounter DSW for breach of privacy information, considers this responsibility an "implied warranty" that companies give their consumers to protect their privacy.

Customers obviously should be able to trust that companies providing products and services to them will secure their credit card and other personal information. If companies fail to do so, customers won't want to continue doing business with those providers. Though the company may lose customers, until recently, the legal standard for corporate responsibility for protecting consumer information has been murky. But as State Attorney Generals start prosecuting companies who fail to secure that data, a new, stricter standard appears to be taking shape, at least as far as those tasked with consumer protection seem to believe.

In addition, businesses are contending with the threat of consumer class-action suits. Attorneys filing suit on behalf of consumers have been able to quantify costs to consumers based on the average expense they would incur if their private information were breached. Companies are paying dearly for security breaches. A Fortune 500 retailer recently settled litigation in connection with inappropriate sharing of personal information to the tune of almost \$60 million.

The FTC's stance on this issue is clear. The commission insists consumers should have confidence that the companies they do business with will protect their sensitive private information, such as credit card data. Because no company thus far has been willing to litigate these issues, thereby challenging regulators' positions, at least in the foreseeable future it would appear that more strict accountability for information security will be the standard of the day.

## Calculating the Costs

### Identify Theft: Costs and Potential Damages

#### FTC Complaints:

2000: 31,000

2001: 86,000

2002: 162,000<sup>1</sup>

2003: 215,000<sup>2</sup>

2004: 247,000<sup>3</sup>

**28 percent of complaints involve credit card fraud**

#### Average Impact of Each Identity Theft:

**\$16,000<sup>4</sup>**

**600 hours of clean up<sup>5</sup>**

#### Other Ramifications: Credit disruptions

Source: FTC Consumer Sentinel and Identity Theft Clearinghouse and the Identity Theft Resource Center.

<sup>1</sup><http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf> (FTC February 1, 2005 study).

<sup>2</sup><http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf> (FTC February 1, 2005 study).

<sup>3</sup><http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf> (FTC February 1, 2005 study).

<sup>4</sup><http://www.idtheftcenter.org/facts.shtml>

<sup>5</sup><http://www.idtheftcenter.org/facts.shtml>  
(Based on 600 hours times the indicated victim wages, this equals nearly \$16,000 in lost potential or realized income.)

Though the actual threat to consumer privacy may not be increasing, consumer complaints are on the rise — and so is the cost. In 2000, 31,000 complaints were filed with the FTC against companies for breach of confidential information; in 2004, that number rose to 247,000.

The average impact of an individual identity theft is \$16,000 with 600 hours of clean up, according to the Identity Theft Resource Center, a national nonprofit organization that focuses exclusively on identity theft. According to an FTC study, credit card, phone, and bank fraud were some of the most common complaints. In addition, the percentage of complaints about electronic fund transfer-related identity theft more than doubled between 2002 and 2004. Further, the overall number and cost is expected to continue to rise each year.

In the aggregate, the consequences can be quite expensive. For consumers, the cost is pegged at about \$5 billion — and for the industry, that number is closer to \$48 billion. Gartner Research estimates that by 2006, 20 percent to 30 percent of the Global 1000 will have to face legal issues for their failure to secure customer information. Gartner estimates that number at \$5 million to \$20 million per business.

As a result, companies literally can't afford to not protect their customer data — and themselves. So whether a company promises to protect consumer information or offers no such guarantee, the company is under legal pressure to guard that data or risk prosecution at a time when the legal standard is fluid. In the same way people lock their doors as a matter of course to protect their homes, companies need to have a policy, a plan, and the necessary tools in place to protect customer data.

## Applying the DRIP Approach

In order to minimize the legal risks, companies should implement an information security program following the DRIP approach: **Designate** responsible employees, assess **risks**, **implement** safeguards, and revise the **program**.

- **Designate Employees Responsible for the Program:** A company's first step in that self-preservation is to assemble a team, which can be a multi-disciplinary task force or a working group made up of employees with a stake in the company's success, to be responsible for information security. That team should include employees with knowledge of both information security and privacy issues. In addition to IT members, the team should include the company's privacy officer, compliance officer, and legal counsel.
- **Regularly Perform Risk Assessments:** Companies need to perform a risk assessment to learn and map their data flows, both within the organization and with vendors. This assessment should identify all risks to the security, confidentiality of corporate trade secrets, and the integrity of customer information, including training, system design, and potential risks. The risk assessment helps organizations close security gaps, but it also provides an ancillary benefit by helping companies institute policies that are both more secure and efficient.
- **Implement Specific Safeguards:** Based on the findings of the corporate risk assessment, the company should institute specific safeguards that address the risks — and monitor and enforce those policies on outbound traffic with an Information Leak Prevention solution.

What many companies will find through a careful study of data flows is that IP leakage — or the outflow of confidential data including customer information and trade secrets through email or instant messages initiated by internal employees — is one of the primary threats to information security today. Gartner Research finds that 80 percent to 90 percent of data exposure incidents resulted from established business processes or employee error.

- **Revise the Program Through Constant Learning:** Rather than approach this effort as a one-time project, companies need to continually revise this program based both on what is going on internally and externally in the marketplace. Companies should automatically enforce these policies for violations as well as audit for compliance.

Executives have an incentive to ensure customer data is safeguarded beyond protecting their company's brand identity. Senior executives within a company are being asked to certify the adequacy of their company's internal controls as of sections 302 and 404 of Sarbanes-Oxley. A deficiency in internal controls may trigger a public disclosure obligation to the SEC. Because the legal climate is so dynamic with respect to corporate responsibility and information security, many clients are choosing to identify the laws with the strictest standards and map their policies and controls to these standards.

For example, California's statute requiring notification of a security breach requires a company to notify consumers whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Consequently, lawyers are advising clients who handle consumer information to make sure that information is encrypted throughout the organization.

Multinational businesses also have to be keenly aware of even stricter and better articulated standards in international law. Laws such as the EU Data Directive, the Canadian Data Protection Law (PIPEDA), and the Japanese Data Directive dictate requirements that in some instances are considerably more strict than the standards in the U.S.

## PortAuthority Protects Against Information Leaks

As businesses face greater scrutiny and more legal responsibility for the manner in which they handle sensitive data, those organizations need to ensure they do everything they can to prevent the leakage of sensitive data. That means understanding the source of the most common breaches and having an automated system in place to enforce policies and plug those leaks. With 70 percent of serious security incidents caused by internal employees, according to Gartner Research, traditional, threat-centric defenses like intrusion prevention systems and firewalls are of little help in stopping the outflow of information.

Information Leak Prevention (ILP), a new category of data security policy enforcement solutions, uses deep packet inspection technology to track and audit private content in-transit. ILP aims to identify materials that are not in compliance with corporate data security policies and prevent their distribution. PortAuthority is the industry's first real-time enforcement solution to use sophisticated fingerprinting technologies to accurately identify sensitive information within the business context and stop breaches.

The PortAuthority platform applies 27 patent-pending identification technologies to analyze network traffic in real time and identify protected content. PortAuthority resists all types of data manipulation, including cutting and pasting, reformatting, retyping, and changing file extensions to protect confidential data from structured, semi-structured, and unstructured sources. It protects data in structured databases like Oracle, Siebel, SAP, and IBM DB2; semi-structured data from email and Web forms; and documents, spreadsheets, files, and other unstructured data, including CAD, PDF, Word, Excel, and PowerPoint. PortAuthority uses contextual analysis to spot fragments and derivations of protected content.

When the PortAuthority platform identifies protected content, it then takes action by tracking, and even preventing, the transmission of that content across network boundaries. The PortAuthority platform enforces information leak prevention across email, Web, and other communications channels.

Businesses can use PortAuthority to enforce internal security and compliance policies, including blocking, quarantining, and encrypting sensitive information. Security policies can be managed by department, group, and content type. PortAuthority is designed to fit into existing business processes and IT environments, and is simple to administer with no client software to manage or end-user training required.

Extensive reporting in the PortAuthority platform offers security professionals visibility into internal sensitive data policy breaches and provides an extremely detailed audit trail they can use to validate their organizations' regulatory compliance.

The PortAuthority solution is ideal for companies that understand the need to stop the leakage of sensitive data, but lack an automated mechanism to do so. With fewer than 25 percent of U.S. companies currently monitoring outbound email content, a tremendous number of organizations are putting themselves — and their executives — at risk.

## Contributing Author: Gerard M. Stegmaier, Esq.

Gerard M. Stegmaier is an attorney with Wilson Sonsini Goodrich & Rosati who practices privacy and data protection law. Mr. Stegmaier also teaches a variety of privacy related courses at George Mason Law School. For the past several years he has served on the Joint Commission on Technology & Science Privacy Advisory Committee of the Virginia legislature where he assists legislators with analyzing and reviewing technology and privacy related legislation. He is a frequent author and speaker on privacy and information security issues and has been involved in a number of the most prominent Internet and privacy-related litigations decided in recent years. The author may be reached at: [gstegmaier@wsgr.com](mailto:gstegmaier@wsgr.com). The views expressed herein are solely the respective authors and do not represent the views of Wilson Sonsini Goodrich & Rosati or any organization with which Mr. Stegmaier may be affiliated.

## Sponsored by PortAuthority Technologies™

PortAuthority Technologies™, the leader in Information Leak Prevention, develops security software that reliably and accurately controls the unauthorized communication of sensitive information. Our solutions help ensure compliance with regulations like Gramm-Leach-Bliley, HIPAA, CA CC1798, PIPEDA and Sarbanes-Oxley by closing the gap between employee behavior and corporate policies. PortAuthority stops leaks of private and confidential information by monitoring enterprise communications and delivering effective policy enforcement in real-time. PortAuthority Technologies is a privately-held company with funding from Greylock Partners, Lexington Ventures, and Sequoia Capital.

**PortAuthority Technologies™**  
**[www.portauthoritytech.com](http://www.portauthoritytech.com)**  
**877.843.4879 Toll-Free**

WP0101-1005