

October 2005

**PRIVACY BREACHES
AND THE
LESSONS LEARNED**

Over the last year, it has been difficult to pick up a newspaper or turn on the news without hearing about another breach of private consumer information. As a result, 2005 will go down in history as the "Year of the Data Breach." Consumers' identity theft fears have escalated and regulators are reacting. On the heels of story after story about companies losing their customers' or employees' personal information via hackers or other lapses in security measures, Federal and state regulators are taking a closer look at how they can increase the regulation of health, personal and financial information. So, there is little doubt 2006 will become the "Year of Privacy Protection Regulations."

Whether through Federal or state legislation, businesses that collect and maintain personal information can be assured that in the near future, a government entity will be placing greater security and privacy requirements on procedures associated with the collection and storage of personal information. Medical and financial institutions have experienced heightened security requirements for several years through legislation such as HIPAA¹ and Gramm-Leach-Bliley.² In July 2005, federal rules were enacted requiring thousands of banks and other financial institutions to notify customers if their private information was obtained by hackers or identity thieves and is likely to be misused. The Federal Deposit Insurance Corp., the Federal Reserve, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision coordinated the enactment of the rules.

Under one of several recent Congressional proposals, Senator Specter's *Personal Data Privacy and Security Act* requires notification of individuals who are affected by a security breach. The legislation provides exemptions for companies that perform a risk assessment and conclude that there will not be any harm to affected individuals. It also exempts companies that participate in a security program designed to block the use of personal information for unauthorized financial transactions.

This is only the first wave of what is certain to be an onslaught of privacy regulations soon to follow. Sure to be coupled with the privacy regulations will be high profile enforcement actions by federal and state regulators. One such action occurred in November 2005 when the Federal Trade Commission (FTC) issued a Final Order against BJ's Wholesale Club, Inc.³ In that Order, BJ's Wholesale Club, Inc. agreed to settle FTC charges that its failure to take appropriate security measures to protect the sensitive information of thousands of its customers was an unfair practice that violated federal law.

¹ Health Insurance Portability and Accountability Act of 1996

² The Gramm-Leach-Bliley Act of 1999

³ *In the Matter of BJ's Wholesale Club, Inc.*, File No. 042 3160

According to the FTC, this information was used by an unauthorized person 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 a period of 20 years.

The groundbreaking aspect of the BJ's Order is that it specifically applied privacy safeguarding standards to a business that was not previously required to follow specific privacy standards. With the issuance of this Order, the FTC has put all companies on notice that if you maintain personal information about consumers, you are required to safeguard the information. No matter if you are a medical provider, financial institution or retail business establishment; you are required to take appropriate measures to ensure that unauthorized persons do not have access to your customers' personal information. The Order requires businesses to establish and maintain a written comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information the business collects from or about consumers. The security program must contain administrative, technical, and physical safeguards appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected. Specifically it requires companies to:

- Designate an employee or employees to coordinate and be accountable for the information security program.
- Identify material internal and external risks to the security, confidentiality, and integrity of consumer information that could result in unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.
- Design and implement reasonable safeguards to control the risks identified through risk assessment, and regularly test or monitor the effectiveness of the safeguards' key controls, systems, and procedures.
- Evaluate and adjust its information security program in light of the results of testing and monitoring, any material changes to its operations or business arrangements, or any other circumstances that the company knows or has reason to know may have a material impact on the effectiveness of its information security program.

In a similar action, consumer data broker ChoicePoint, Inc. agreed to resolve issues surrounding the unauthorized access to more than 163,000 consumer personal finance records by agreeing to pay the FTC \$10 million in civil penalties and consumers \$5 million in restitution. ChoicePoint agreed to: 1) implement new procedures to ensure that it provides consumer reports only to legitimate businesses for lawful purposes. 2) Establish and maintain a comprehensive information security program designed to protect the personal consumer information it collects, and 3) obtain a third-party independent

audit every two years for a period of 20 years to ensure that its security program meets the standards it agreed to abide by with the FTC.

The FTC and regulators in general are focusing a significant amount of resources in privacy enforcement. It is more important than ever that these companies understand what requirements apply to their organizations, how to comply and what steps to take in the event of a breach. The significant regulations in this area are as follows.

HIPAA

On February 20, 2003, the final HIPAA Security Standards were published. The Security Standards establish detailed requirements for safeguarding patient information that is electronically transmitted or stored. The rule establishes 42 implementation specifications, 20 of which are “required,” meaning they must be implemented as specified in the rule. Twenty-two are “addressable.” Complying with addressable implementation specifications requires a business to assess whether they constitute a reasonable and appropriate safeguard for the particular business; if not, an alternative approach must be designed and implemented to achieve the particular standard.

HIPAA’s Security Standards are probably second nature to the “covered entities” (CEs) to which HIPAA applies⁴. There are many questions about notification requirements under HIPAA. HIPAA does not specifically require that a CE notify patients when Protected Health Information (PHI) is improperly disclosed; however, HIPAA does require CEs to “mitigate” the damage caused by the improper releases of PHI. Informing patients of an improper release of PHI may be required as part of mitigation. The decision to inform patients as part of mitigation is a very fact specific determination and a privacy attorney should be consulted to assist in this decision. The HIPAA evaluation does not end the discussion. CEs need to know to what extent state laws are applicable, particularly in the event of a breach.

STATE PRIVACY & NOTIFICATION LAWS

As is typical of consumer protection laws, the states are leading the regulatory charge. Most states have enacted regulations which impose confidentiality requirements on medical records. A state-by-state regulatory structure has emerged since 2003 when California passed one of the first laws requiring notification of data theft or loss. Since 2003, over 20 states have enacted similar laws and many more states have privacy bills pending. New York’s law is one of the more onerous regulations. It requires companies to disclose any unauthorized breach of databases that contain the unencrypted personal information of New York residents without any exceptions for small data breaches or breaches that are unlikely to result in identity theft. Furthermore, there is no exception for companies that have their own disclosure policies.

⁴ For a summary of HIPAA’s privacy protections visit: <http://www.hhs.gov/news/facts/privacy.html>

State regulations in this area generally share three common points. They require companies to:

- notify consumers nationwide if certain types of breaches occur
- set minimum standards for security
- impose stiff civil and/or criminal penalties for violations

ADVICE FOR PROTECTING YOUR COMPANY

Protect your company by reviewing your privacy policies and ensuring you have adequate security procedures in place. Now is the time to start conducting audits assessing how well your organization secures your customers' and employees' private information. When conducting your audit, keep in mind the overwhelming majority of data breaches are the result of "low tech" breaches such as employee theft or unsecured physical files. If your audit reveals flaws in your policies, procedures or security systems, then make improvements immediately.

In the meantime, here are some general suggestions for safeguarding confidential information:

- **Data Security** – develop policies and procedures and conduct training regarding data security to include:
 - Requiring employees to log off of unattended computers.
 - Implementing a password protocol and requiring that passwords not be shared or disclosed to unauthorized individuals.
 - Installing and routinely running anti-virus software and updating your operating system on a regular basis with the latest security patches, updates and drivers. This will ensure your computer is up-to-date and will help prevent against viruses and other security breaches.
 - Maintaining the confidentiality of all data, keeping in mind the privacy of all individuals.
 - Protect confidential data files through encryption.
- **Document Destruction** – dispose of confidential information in a secure manner.
- **Facility Security** – ensure that no unauthorized individuals have access to facilities.
- **Outsourcing/Subcontractors** – inquire about their security protocols and if they meet standards, insist on strict compliance.
- **Employee hiring** – conduct background screenings and have employees sign privacy statements.

Most importantly, hire a compliance officer or assign compliance officer duties to a current employee. Stay current on privacy regulations and revise and adopt your privacy policies and procedures accordingly.