

December 2005

Protecting Your Customer's (and Your Business) Interests

Late 2005, the Federal Trade Commission (FTC) entered into a settlement agreement with B.J. Wholesale (B.J.'s).

The FTC sued B.J.'s after a data breach of B.J.'s customers' credit card information. As a result of the data breach, several million dollars in fraudulent purchases were made using counterfeit copies of credit and debit cards members had used at BJ's stores. The counterfeit cards contained the same personal information BJ's had collected from the magnetic stripes of members' credit and debit cards and then stored on its computer networks.

The complaint alleged that BJ's stored members' personal information on computers at its stores and failed to employ reasonable and appropriate security measures to protect the information. The complaint also alleged that this failure was an unfair practice because it caused or was likely to cause substantial consumer injury that was not reasonably avoidable and was not outweighed by countervailing benefits to consumers or competition. The specific allegations were that BJ's (1) failing to encrypt information collected in its stores while the information was in transit or stored on BJ's computer networks; (2) storing the information in files that could be accessed anonymously, that is, using a commonly known default user id and password; (3) failing to use readily available security measures to limit access to its networks through wireless access points on the networks; (4) failing to employ measures sufficient to detect unauthorized access to the networks or conduct security investigations; and (5) storing information for up to 30 days when BJ's no longer had a business need to keep the information, in violation of bank security rules.

In its settlement with B.J.'s, the FTC required B.J.'s to establish and maintain a comprehensive information security program in writing that is reasonably designed to protect the security, confidentiality, and integrity of personal information it collects from or about consumers. The security program must contain administrative, technical, and physical safeguards appropriate to BJ's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected. Specifically, the order requires BJ's 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 BJ's knows or has to reason to know may have a material impact on the effectiveness of its information security program.
- Conduct a biennial assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that: (1) BJ's has in place a security program that provides protections that meet or exceed the protections required by Part I of the proposed order, and (2) BJ's security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of consumers' personal information has been protected.
- Submit compliance reports to the FTC

As a result of the B.J.'s decisions, all companies that collect consumer information are required to follow security safeguards rule that previously are applied to financial institutions through the Graham-Leach-Bliley Act. The rule, commonly called "The Safeguards Rule" requires financial institutions to take reasonable measures to safeguard confidential consumer information. The rule focuses on three areas:

1. Human Resources (i.e. hiring practices confidentiality policies and procedures).
2. Technology (encryption, secure transmissions).
3. Facilities.

The FTC now requires regardless of industry and formal statutory or regulatory requirements, must maintain an effective data and information security program. So, if you collect or maintain personal information, you must have such a program.

The B.J.'s decision is a wakeup call for companies to enact policies and procedures to protect confidential customer information.