

Legal Review: Preparing Your Company for a Data Breach

Dec 1, 2006

By: [Linda A. Goldstein](#), [Angela C. Hurdle](#)

Response



Linda A. Goldstein

It seems that each day, another company is reporting a breach of its customers' personal information. Data security is becoming an increasing priority for all companies, especially for direct response marketers, for whom the use and collection of consumer information is of primary importance.

Since February 2005, there have been more than 330 data loss incidents, exposing more than 94 million individual records. However, data breaches are not just a consumer problem. A recent study that surveyed 56 companies about their data breach experiences in the past year found that, on average, each company suffered a loss of \$4.7 million, including \$2.5 million in lost business.

Although there are numerous pending federal bills addressing data breaches, none have been passed. Therefore, companies are currently subject to a multitude of state laws, as well as the threat of Federal Trade Commission (FTC) or other regulatory action. Though five years ago, the FTC was concerned with companies that breached their privacy policies regarding the use, protection and disclosure of consumers' personal information, within the past year we have seen a shift in the Commission's focus.

In the past five years, the FTC has brought 13 cases against companies under Section 5 of the FTC Act, which prohibits unfair and deceptive trade practices. The FTC's position is that failure to take reasonable steps to protect sensitive consumer data is an unfair business practice.

Companies started paying attention when the FTC settled with ChoicePoint Inc. in early 2006 for \$10 million. When records of more than 163,000 consumers in its database were compromised, the FTC charged that ChoicePoint's security and record-handling procedures violated consumer's privacy rights and federal laws.



Angela C. Hurdle

In March, DSW Inc., a discount shoe retailer settled charges with the FTC for its alleged failure to reasonably protect customer data. As a result of lax data protection measures, hackers allegedly accessed the financial information of more 1.4 million DSW customers, resulting in several cases of identity theft. The FTC alleged that DSW engaged in practices which, taken as a whole, were considered unfair.

The FTC's settlement with DSW provides useful guidelines. The Commission has held that its Safeguards Rule provides model corporate behavior for all businesses and requires that

companies develop a written information security plan that describes their program to protect customer information.

Each company must: (1) designate one or more employees to coordinate safeguards; (2) identify and assess risks to customer information in each relevant area of the company's operations, and evaluate the effectiveness of current safeguards; (3) design and implement safeguards program, and then regularly test and monitor it; (4) select an appropriate service provider and contract with them to implement safeguards; and (5) evaluate and adjust its plan in light of relevant circumstances including changes in business or results of testing or monitoring.

As of July 2006, approximately 33 states have enacted security breach notification laws applicable to companies in possession of consumer personal information. These laws generally require that companies take all reasonable steps to destroy consumers' personal information once the company no longer has a business need for such information; establish reasonable security procedures and practices appropriate to the nature of the information; require, by contract, with any third parties, that such party establish reasonable security practices; and upon discovery, disclose any breach to consumers whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Direct response marketers must also address any third parties that have access to their customers' personal information. Joint marketing and cross-selling agreements should contain appropriate provisions requiring the third party to maintain certain security measures.

While many direct response marketers have recently begun encrypting data in order to comply with Visa and MasterCard requirements, it is important to note that encryption and/or PCI compliance will not insulate a company from enforcement action in the event that a data breach occurs. Direct response marketers should take a comprehensive look at their data security policies and procedures, ensure that a written incident response plan is in place and conduct frequent auditing and monitoring to ensure that its policies and procedures are being followed.

Linda A. Goldstein is a partner and Angela C. Hurdle is an associate in the New York office of Manatt Phelps & Phillips LLP. They can be reached via E-mail at lgoldstein@manatt.com and ahurdle@manatt.com respectively.