Paul Hastings
ATTORNEYS

January 2006

StayCurrent
A Client Alert from Paul Hastings

Ushering in 2006: FTC Not Waiting for Congressional Action on Data Security

Behnam Dayanim and Kristine A. Rembach

The Federal Trade Commission's recent consent decree with shoe discounter DSW Inc. represents the Commission's broadest exercise of authority in the area of data security and sends a clear signal that the FTC is willing to take action even in the absence of a specific statutory data security mandate.

The DSW Case

DSW collected a variety of personal information, including names, credit card numbers, security codes, checking account numbers, and driver's license numbers, from customers purchasing merchandise from DSW stores. That personal information was transmitted via wireless internet to an in-store computer network, then transmitted via internet to the company's corporate computer network. The FTC alleged, among other things, that DSW stored the information long after the company no longer had a business need for it and failed to utilize readily available security measures to limit access to consumers' personal information via the wireless access points in its stores. The FTC claimed that this lapse compromised approximately 1.4 million credit and debit card numbers and 96,000 checking account or driver's license numbers, resulting in authorized charges and other harm.

As part of the consent decree, DSW agreed to implement a comprehensive information security program and to commission audits by an independent security professional every other year for 20 years. DSW also will be subject to standard FTC record-keeping and reporting requirements that will allow the FTC to monitor DSW's compliance with the settlement agreement.

The Legal Basis for Pursuit of DSW

The FTC based its claims against DSW on its existing statutory authority, provided under the FTC Act. That act prohibits "unfair trade practices." In prior actions involving data security breaches, the FTC tied its authority to specific, allegedly false representations made by the company regarding its own data security measures – for example, an untrue claim that its customer information was encrypted.

However, with DSW, the FTC seemed to assert that the statute's "unfair trade practices" proscription impliedly requires companies collecting sensitive personal information from consumers to employ reasonable safeguards to protect the security of that information. The FTC previously imposed such a requirement on financial institutions, through enforcement of the Safeguards Rule under the Gramm-Leach-Bliley Act, which became effective in 2003. However, that rule was enacted pursuant to a specific statutory directive affecting certain categories of financial institutions. The DSW case is not tied to any sector-specific statutory authority.

Whether the FTC's expansive interpretation of the FTC Act in this area would be vindicated if challenged is uncertain. Companies facing FTC complaint on these issues face a strong incentive to negotiate, rather than to litigate. As a result, judicial resolution of this question may not soon be forthcoming.

Congressional Action on Data Security

As we reported in a recent client alert, "Data Protection Legislation Moves Forward in the Senate: Increased Congressional Activity Expected this Fall" (August 24, 2005), the U.S. Congress has focused much attention on data security measures this past year. The FTC has testified in connection with many of these initiatives, and several of the introduced bills would vest the FTC with specific enforcement authority in this area.

Several congressional committees, including the Senate Commerce Committee, Senate Judiciary Committee, and House Energy & Commerce Committee, among others, have passed or are considering bills that would require companies that collect sensitive information from consumers to implement data security safeguards and to notify consumers of breaches. The measures have been slowed by debate among committees and as a result of turmoil over other, unrelated matters. Moreover, in the House, some partisan differences have emerged. Nevertheless, we expect that Congress will agree on and pass a data security bill within the first half of the new year.

Paul Hastings' Privacy and Information Security Practice advises clients on all aspects of privacy and information security law and regulation, conducts privacy assessments, formulates and helps establish privacy and security compliance programs, and represents clients facing privacy enforcement investigations or litigation. We also represent clients in working with Congress and the Federal regulatory agencies in the formulation and implementation of public policy in this dynamic and important area. Behnam Dayanim is a partner and Kristine Rembach is an associate in Paul Hastings' Washington, DC, office. For more information on the subject of this alert or on any other privacy or information-security related topic, please contact:

Behnam Dayanim (202) 551-1737
bdayanim@paulhastings.com

Michael Lindsey (213) 683-6262
michaellindsey@paulhastings.com

Robert L. Sherman (212) 318-6037
robertsherman@paulhastings.com