

# FTC Settles With Sears Over the Company's Online Tracking Software

June 17, 2009

On June 4, 2009, the Federal Trade Commission (FTC) announced a settlement with Sears Holdings Management Corporation (SHMC) – owned by Sears, Roebuck and Company and Kmart Management Corporation – over allegations that the company failed adequately to disclose the scope of information it collected about consumers by means of a downloadable software application.

While SHMC did disclose, in the installation process, outside the privacy policy, that the application would track "online browsing," the FTC alleged that the disclosure was not sufficient to describe all of the tracking activities that the program performed. Through this high-profile case against a nationally-recognized company, the FTC appears to be ratcheting-up its call that material information should be disclosed prominently outside of the Privacy Policy and in a way that consumers can understand the full consequences of the disclosure.

## Complaint

According to the FTC complaint, from approximately April 2007 to January 2008, SHMC used pop-up messages to invite consumers visiting sears.com and kmart.com web sites to become members of "My SHC Community." Consumers who accepted the invitation and provided their e-mail addresses would then receive an e-mail inviting them to join the "online community," in exchange for downloading a tracking application to their computers for at least one month. Consumers who retained the application for that time period would receive \$10 in compensation.

SHMC disclosed in paragraph four, sentence three of the invitation e-mail that the downloaded application would "confidentially track [consumers'] online browsing." Consumers who accepted the e-mail invitation were directed to a landing page, where they were asked to re-confirm their intent to join.

Those who accepted were then directed to a registration page which, in addition to asking for additional consumer information, contained a privacy policy that disclosed the specific functions of the application. The functions disclosed in the privacy policy included that the application would monitor consumers' online secure sessions and sessions on third party web sites, as well as information transmitted in those sessions, such as the contents of shopping carts, online banking statements, video rental transactions, library borrowing histories, online drug prescription records, and select header fields that show the sender, recipient, subject, and size of web-based e-mail messages.

The FTC alleged that the disclosure outside of the Privacy Policy and User License Agreement **was not prominent enough nor specific enough** and was therefore deceptive and in violation of Section 5(a) of the FTC Act.

## Settlement Agreement

The proposed settlement agreement requires SHMC to stop collecting data from any tracking application within three days and to destroy all data collected by any tracking application within five days. SHMC is also required to notify all consumers that installed the tracking application to inform them what the application does and how to uninstall it.

Additionally, the agreement requires that, going forward, SHMC:

1. clearly and prominently disclose the specific functions of any tracking application prior to the display of, and on a separate screen from, any privacy policy or similar document; and
2. obtain express consent from the consumer to download or install a tracking application and collect consumer data.

The agreement imposes a four-year record-keeping requirement and requires the company to furnish, on request, all documents related to complaints, inquiries, terms and conditions, or advertisements associated with any tracking application to the FTC. The proposed settlement agreement will be subject to public comment for 30 days, through July 6, 2009.

## Kelley Drye & Warren LLP

Kelley Drye & Warren's [Privacy and Information Security](#) practice is a leader in advising clients on privacy and information security issues and has been at the forefront of developments in this growing area of the law. Our attorneys regularly counsel clients regarding all aspects of privacy and data security compliance, including drafting and amending privacy and information security policies, advising clients on interpreting their own policies, crafting data security programs for clients, performing privacy and/or data security audits of existing business practices, drafting agreements with third parties regarding their obligations in connection with handling clients' customer data, and representing clients in connection with federal and state regulator privacy investigations regarding their privacy and data security practices.