InsideCounsel.com
BUSINESS INSIGHTS FOR LAW DEPARTMENT LEADERS
September 13, 2013


Technology: 5 Things to know now about the FTC and data security

The commission advances its ongoing effort to make companies responsible for protecting the privacy and security of consumer data

BY RICHARD MARTINEZ, MELISSA GOODMAN

August 2013 saw two significant developments in the Federal Trade Commission's (FTC) ongoing efforts to make companies responsible for protecting the privacy and security of consumer data. First, the FTC announced that it had brought an administrative action against LabMd, a medical testing company that performs lab tests on patient samples provided by physicians. The FTC alleges that LabMd's failure to take adequate and reasonable security measures resulted in the unauthorized disclosure of private consumer information including names, Social Security numbers, dates of birth, health insurance provider information, bank account information and standardized diagnostic codes for medical procedures. Second, TRENDnet, the maker of an Internet-connected home security video camera, settled charges the FTC had brought against it after hundreds of its customer's private home security video feeds were made public on the Internet. The key insights these cases reveal can help inside counsel understand both the current risks associated with a data breach of consumer information and the best ways to avoid data privacy-related scrutiny from the FTC – and the attendant media spotlight that could follow.

1. The FTC uses the FTC Act to police U.S. business data security standards.

Section 5 of the Federal Trade Commission Act (FTC Act), 15 U.S.C. § 45, prohibits "unfair or deceptive acts or practices in or affecting commerce." When it comes to data security, the FTC invokes its power to police deceptive practices if a company breaches or disregards its own published policies or statements regarding data privacy. In order to justify its involvement because of unfairness, the challenged data security practice must substantially harm or threaten to harm consumers and the threatened harm must outweigh any possible benefits. The FTC uses its authority to pursue companies that fail to provide reasonable and appropriate data security practices. The complaint against LabMd—which has not yet been made public because it contains information that LabMd claims is confidential—is based on unfairness. The TRENDnet complaint included both unfairness and deceptive practice allegations.

2. The FTC's power to regulate data breaches caused by third parties is disputed.

Despite having brought and settled over 40 data security cases, the FTC's power to bring data security cases for breaches caused by third parties under its unfair and deceptive trade practices authority has not been fully established. When the FTC first began investigating LabMd, LabMd refused to comply with the FTC requests for information and the FTC sought a court order. The district court agreed with LabMd that the FTC's power under the unfairness category is not unlimited. The court ultimately rejected LabMd's attack on the FTC's authority, however, because the FTC investigatory authority only needs "a plausible argument" for jurisdiction. The court found that the FTC had met that standard for the investigation phase. But LabMd has indicated that it will challenge the FTC's authority under Section 5 of the FTC Act.

And then there's the battle between the FTC and the Wyndham hotel chain. Various allegedly lax data security policies and procedures at Wyndham hotels led to three data breaches of customer information in an 18-month period, resulting in over a half-million credit card records ending up in the hands of identity theft rings in Russia. After the FTC filed an enforcement action against Wyndham in district court, Wyndham moved to dismiss, challenging the FTC's authority to bring an action based on security breaches caused by a third party. Among its arguments, Wyndham said it lacked sufficient notice because the FTC has not published any rules or regulations explaining what data security practices a company must adopt to be in compliance with Section 5 of the statute. Wyndham also argued that specific acts like the Fair Credit Reporting Act, the Children›s Online Privacy Protection Act, the Health Insurance Portability and Accountability Act, and the Cable Television Consumer Protection and Competition Act have given the FTC power over data security in these specific areas, but foreclose a broader statutory authority over data security standards in general. A decision on Wyndham's dismissal motion is imminent.

3. Even though the FTC has yet to promulgate any regulations on data privacy, enforcement activity has developed some data practice guidelines.

Analysis of the complaints filed against TRENDnet, LabMd--and others--reveal the kinds of conduct the FTC considers to be "unfair" when it allows third parties to access a consumer's private information. Challenged conduct includes:

- Failure to implement or maintain a comprehensive data security program to protect consumer information through the use of readily available measures, including things like firewalls and employee training;
- Permitting improperly-configured software to display password, financial information, or login information in unencrypted clear text;
- Failure to ensure and maintain security across user networks;
- Failure to follow best practices for password complexity;
- Failure to employ reasonable measures to detect and prevent unauthorized access;
- Failure to use reasonable security to design and test privacy-sensitive software;
- Improper use of peer-to-peer networks;
- Failure to follow proper procedures to prevent repeated intrusions; and
- Failure to restrict third-party access to data networks.

Companies who adhere to data practices that address these concerns have the best

[InsideCounsel].com
BUSINESS INSIGHTS FOR LAW DEPARTMENT LEADERS
September 13, 2013

Technology: 5 Things to know now about the FTC and data security

defense against FTC involvement should a data breach occur. Additionally, take the time to review your company's privacy policy to make sure the FTC won't later argue that you are not honoring the promises you've pledged.

4. It's time to understand the Internet of Things because the FTC does and intends to regulate the data concerns it implicates.

Smart appliances from phones to bathroom scales, thermostats, refrigerators and wristfitness monitors transmit a steady stream of personal data to manufacturers, service providers, and others. The FTC has significant concerns that a smart technology's inadequate security can allow private information to be revealed in a way the consumer never intended. The result is a November 2013 Internet of Things Workshop the FTC will hold to address the unique issues associated with smart technology—and the enforcement action against TRENDnet, whose unsecure internet-run security system serves as an early object lesson to others in the Internet of Things arena.

5. The potential bad publicity is a good reason to take all practical data security measures you can.

FTC scrutiny generally, and enforcement actions in particular, can result in public relations disasters. Imagine the impact of media scrutiny accompanying an FTC action that alleges your company's product or service jeopardized consumer privacy. Those allegations—coming from a government consumer watchdog—carry much more potential reputational risk than class action allegations coming from private litigants. As a result, they may lead to even greater negative publicity. And publicity directed at one allegedly unsecure device could cast a cloud over other products made by the same company.

Data breaches involving consumer data also don't just earn bad headlines—they can engender consequences like the consent decree TRENDnet entered into with the FTC. In addition to its other settlement obligations, TRENDnet's settlement requires it to participate in 20 years of annual FTC audits as a consequence of it inadequate protection of consumer's private data.

About the Authors

Richard Martinez

Richard Martinez is a trial attorney at Robins, Kaplan, Miller & Ciresi L.L.P. Rick's practice focuses substantially on technology, primarily in the areas of intellectual property litigation. His practice is also active in matters before the International Trade Commission, and in the areas of cyber security, data privacy, and information law.

Melissa Goodman

Melissa Goodman is a trial attorney at Robins, Kaplan, Miller & Ciresi L.L.P. Her experience includes complex business disputes involving contracts, intellectual property, unfair competition, trade secrets and fraud actions. Contact her via email at magoodman@rkmc.com.