Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

FTC Steps Up Privacy Enforcement, With No Slowdown In Sight

By **Allison Grande**

Law360, New York (July 23, 2014, 7:36 PM ET) -- Despite facing a pair of court challenges to its authority, the Federal Trade Commission spent the first half of 2014 aggressively pursuing companies such as Snapchat Inc. and Fandango LLC over allegedly misleading privacy promises and lax data security, and attorneys expect the regulator to continue to put pressure on companies to secure and protect the consumer data they hold.

During the first six months of the year, a pair of enforcement actions that the commission initiated in 2012 against Wyndham Worldwide Corp. and in 2013 against LabMD Inc. intensified as the companies pushed courts to find that the FTC lacked the regulatory authority to police private companies' data security under the unfairness prong of Section 5 of the FTC Act.

This, however, did not slow the regulator's efforts to hold companies accountable for alleged privacy shortcomings. The commission since January has announced new settlements with companies including Snapchat, Fandango and Credit Karma Inc. and approved the final versions of previously announced pacts with Accretive Health Inc., Aaron's Inc. and others over allegedly deceptive privacy practices and inadequate security.

And with a New Jersey federal court affirming the regulator's authority to bring data security cases under Section 5 of the FTC Act in an April ruling that refused to nix the Wyndham suit, attorneys don't expect any letup in the second half of 2014.

"We currently have the perfect storm: Many companies are managing troves of data, but only recently has it become clear what the consequences are when mishandling data," Davis Wright Tremaine LLP attorney Sanjay Nangia said. "And recently, the FTC's authority in this context was confirmed in the Wyndham case. These factors suggest an active rest of 2014 for the FTC."

FTC watchers' attention in the first half of the year has mostly been focused on the developments on the Wyndham and LabMD cases, which are now beginning to produce significant rulings.

"There have been other privacy settlements, but the major thing that people who follow the FTC have been looking at is the Wyndham case," Edwards Wildman Palmer LLPpartner Edward F. Glynn Jr. said. "The case is of incredible importance not only to companies that have to deal with the FTC but also to the commission's future enforcement policy."

The administrative proceeding against LabMD, which is currently being heard before an administrative

law judge, has also been on attorneys' radar not just because it represents the second challenge to the FTC's data security authority but also because it raises for the first time whether the commission has the ability to pursue data security actions against entities already regulated by the Health Insurance Portability and Accountability Act.

"In the non-HIPAA sense, health data remains a top concern for the FTC, and it's shown through the LabMD case that it's going in the direction of using its authority against health companies," said Morrison & Foerster LLP partner Andrew Serwin.

The Third Circuit is currently mulling over the district court's affirmation of the commission's security authority and the LabMD proceeding stalled due to a congressional investigation into a key witness. While the outcome of both cases could significantly affect the commission's future privacy enforcement efforts, the first half of 2014 demonstrates that the commission won't back down from its aggressive pursuit of allegedly faulty privacy practices until it is definitively told that its power is invalid.

"To me, the FTC's work in the first half of 2014 has been more about security than privacy — both in advocating for its ability under Section 5 to regulate security in the Wyndham and LabMD cases, and in testifying to Congress in favor of data security legislation," said Kurt Wimmer, the co-chairman of Covington & Burling LLP's global privacy and data security practice group.

In addition to sending FTC Chairwoman Edith Ramirez to testify before Congress on three occasions about data security in the wake of high-profile breaches at Target Corp. and other retailers, the commission also used its existing deception and unfairness authority under Section 5 to respond to other significant recent consumer data breaches.

The commission announced one of its most significant actions in May, when it revealed that popular mobile messaging app Snapchat had agreed to resolve the regulator's claims that it made false promises about the disappearing nature of messages on its app, the amount of personal data the company collected and the strength of its data security.

According to the FTC's complaint, Snapchat not only made multiple misrepresentations to consumers about the functionality and security of its app that stood "in stark contrast" to how the product actually functioned, but it also failed to adequately secure its "Find Friends" feature, a shortcoming that the commission claims resulted in a security breach that enabled attackers to compile a database of 4.6 million Snapchat usernames and phone numbers.

"The Snapchat case is an important reminder for everyone to use common sense and be smart about new technologies," said Kirk Nahra, Wiley Rein LLP's privacy practice chair. "Promises and commitments that may seem hard to believe often are not accurate. The FTC's action was an important action to reinforce the necessity of getting these technology commitments correct."

The commission's action against Snapchat built on several other pacts that the regulator reached or finalized during the first half of 2014, including a consent decree announced in March that resolved claims that Fandango and Credit Karma failed to take reasonable steps to secure their mobile apps and a pact approved in February settling charges that Accretive unfairly exposed sensitive consumer information to the risk of theft or misuse because of its inadequate data security measures.

Kelley Drye & Warren LLP partner Alysa Hutnik noted that the resolutions clearly reflect two of the commission's major themes in privacy enforcement so far this year: flawed notice and consent and

faulty data security by design.

"These cases are a good reminder in how privacy and security by design reviews in the initial stages of development, before going to market, and in connection with product updates, can materially reduce a company's risk of FTC enforcement," she said.

The FTC also signaled its discomfort with business practices that could be perceived as surprising or creepy in suing the operators of Jerk.com in April for allegedly failing to inform users that the site harvested most of its data from Facebook and in approving a final order in March settling charges that Aaron's allowed franchisees to install software on rental computers that secretly monitored consumers.

The regulator also sent an unexpected warning to companies in announcing its 50th settled data security case in January, according to attorneys. In that case, GMR Transcription Services Inc. agreed to settle the FTC's claims that its failure to adequately monitor the contractors it hired to transcribe audio files unfairly exposed consumers' personal and medical data on the open Internet.

"The settlement left no doubt that companies are responsible for properly managing their vendors and subcontractors, and that simply signing a contract that shifts liability to a vendor or subcontractor does not eliminate that liability," Davis & Gilbert LLP partner Gary Kibel said.

Attorneys anticipate that the FTC will continue to aggressively pursue data security targets in the second half of the year in order to help stem the tide of data breaches plaguing companies and consumers.

"Given the number of recent, high-profile data security breaches, including those involving Target and Neiman Marcus, the increased number of data breaches in 2013, a trend which is likely to continue, and an increased consumer awareness of data breaches, it is likely that the FTC will continue to take an active stance in seeking avenues to involve itself in data security," said Christopher Nucifora, the chair of Kaufman Dolowich & Voluck LLP's technology services practice group.

Attorneys also predict that the FTC will continue to use nonenforcement tactics, such as the data broker study that the commission released in May and the three-part seminar series that explored issues such as mobile device tracking and the use of consumer-generated health data, to supplement its enforcement tactics, with attorneys specifically flagging a planned Sept. 25 workshop on the potential for big data analytics to disadvantage vulnerable communities.

"The FTC's mandate is to protect consumers, and part of that is education to ensure that organizations are as sophisticated as they should be," Jackson Lewis PCshareholder Amy Worley said. "So I don't see any reason why the commission wouldn't continue to keep bringing enforcement actions while doing education, which provides a good opportunity for businesses to see what the FTC is thinking."

--Editing by Katherine Rautenberg and Richard McVay.
