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 Data Security Authority Remains Murky Despite Wyndham

Law360, New York (April 08, 2014, 2:44 PM ET) -- In the latest and most important federal court decision on data security enforcement, District of New Jersey Judge Esther Salas broadly upheld the Federal Trade Commission's authority to police data security under the "unfairness" prong of Federal Trade Commission Act Section 5. The April 7, 2014, ruling denied Wyndham Worldwide Corp.'s motion to dismiss the FTC's complaint alleging unfair and deceptive data security practices after Wyndham-branded hotels experienced multiple data breaches.

Only weeks earlier, LabMD Inc. — which has been the subject of a similarly long-running administrative action by the FTC arising out of a data breach — filed a lawsuit and a motion for preliminary injunction in an attempt to stop the FTC's administrative litigation against the company. Although LabMD lost its prior bid to dismiss the complaint at the administrative level in January 2014, Administrative Law Judge D. Michael Chappel granted LabMD's February 2014 request to uncover via deposition how the commission formed its allegations that LabMD violated the FTC Act.

Despite the Wyndham decision, the FTC's continued reliance on case-by-case adjudication (rather than rulemaking) to apprise companies of their data security responsibilities has been controversial in some quarters, with commentators complaining that the FTC is applying ill-defined "unfairness" standards under Section 5 in many of these cases. Indeed, the FTC's increased enforcement trend comes at a time when the National Institute for Standards and Technology has sought to establish more consistent voluntary standards regarding data security through its release of the cybersecurity framework.

LabMD's challenge and the Wyndham ruling also follow on the heels of the FTC's testimony before Congress in which the commissioners appealed to Congress for legislative authority to police data breaches. Thus, on the one hand, the FTC is proceeding as though it has the authority to regulate under Section 5, while on the other asking for express data security powers to be delegated to the FTC through new laws.

At the same time, other agencies have jumped into the data security fray — such as the U.S. Department of Defense, which has started a rulemaking process and issued a report regarding cybersecurity regulations governing federal procurements — creating further uncertainty for organizations. It remains to be seen how the FTC's authority will evolve, but it is clear that businesses must continue to follow the frequent movements in this space and be prepared to address evolving compliance requirements.

Wyndham Background

Wyndham and its subsidiaries own and manage franchised Wyndham hotels throughout the United

States. From 2008-2010, hackers allegedly operating out of Russia gained unauthorized access to Wyndham's computer network and accessed specific property management systems on three separate occasions.

According to the FTC complaint, the hackers accessed over half a million unique payment card accounts along with associated names and security codes. These account numbers were exported to a domain registered in Russia. Fraudulent charges on the compromised card accounts totaled over $10 million. The FTC filed its complaint on June 26, 2012, alleging that Wyndham's failure to enact reasonable data security policies constituted an unfair trade practice, and that its published online privacy policy was "deceptive."

Wyndham moved to dismiss the complaint in federal court on three grounds: (1) that the FTC Act does not authorize the FTC to enforce data security standards; (2) that fair notice requires the FTC to promulgate regulations before bringing unfairness claims; and (3) that the FTC's allegations were pleaded insufficiently to support either an unfairness or deception claim. Following extensive briefing from the parties and amici curiae, as well as oral arguments in November 2013, Judge Salas rejected all of these arguments.

First, the court ruled as a matter of law that FTC Act Section 5 empowers the FTC to regulate data security. Despite express congressional delegation of data security regulatory authority to other agencies, "the FTC's unfairness authority over data-security can coexist with the existing data-security regulatory scheme."

Second, the court explained that "the FTC does not necessarily need to formally publish rules and regulations [governing unfair data security practices] since the proscriptions in Section 5 are necessarily flexible." The court also noted that the FTC had provided adequate notice to companies through its public statements, complaints, and published consent orders. Finally, the court held that the FTC had sufficiently alleged how Wyndham's data security practices were unfair and deceptive.

LabMD Background

Like the Wyndham complaint, the FTC's Aug. 29, 2013, administrative complaint against LabMD, a clinical lab testing company, alleged that LabMD failed to implement reasonable and appropriate measures to prevent unauthorized access to consumers' personal computer data, and that this failure resulted in identify theft and disclosure of sensitive medical information.

According to the FTC, LabMD failed to safeguard consumers' personal information in a number of ways, including, but not limited to, the failure to adequately train employees in protecting sensitive information, the absence of a comprehensive security program, and the lack of readily available measures to detect or prevent an unauthorized breach. The FTC further alleged that these inadequate security procedures exposed the personal information of thousands of LabMD customers on two separate occasions in 2012.

In January 2014, LabMD moved to dismiss the complaint on two grounds: (1) that it was not subject to FTC authority because the Health Insurance Portability and Accountability Act alone dictates privacy and security requirements; and (2) that application of the FTC Act to data protection practices without formal rules and regulations violated due process. The administrative law judge rejected both arguments, affirming the FTC's broad jurisdiction to regulate evolving conduct that could harm consumers.

Much like the decision in Wyndham, The ALJ rejected the former argument on the basis that, despite HIPAA standards, the FTC has independent authority to police data security under the FTC Act. The ALJ also affirmed that the FTC is not required to enforce Section 5 via rulemaking processes in place of its long established case-by-case adjudication approach.

Evolving Unfairness Jurisdiction

The Wyndham and LabMD cases illustrate the FTC's evolving and aggressive application of its somewhat amorphous "unfairness" jurisdiction to the area of data security. Under the traditional formulation of the unfairness prong of Section 5, the FTC seeks to show that allegedly lax data security practices inflicted substantial consumer harm that was not reasonably avoidable by consumers, and that the harm was not outweighed by countervailing benefits to consumers. The inquiry necessarily requires the FTC to weigh the pros and cons of constantly evolving security measures, a task that critics have argued the FTC is ill-equipped to handle.

Challenges to Data Regulation Authority

Despite the FTC's strong assertion of authority, the debate regarding the FTC's role in regulating data security continues to evolve in both judicial channels (including the Wyndham and now LabMD challenges in federal court) and legislative avenues (including through proposed legislation and congressional hearings). Though the FTC has been asking Congress for an express statutory authority to regulate data security, the two cases have thus far affirmed that data security already falls within FTC's existing Section 5 jurisdiction.

Notwithstanding the Wyndham decision upholding the FTC's legal authority to regulate data security, companies such as LabMD and Wyndham still argue that they should not be held to security standards that have not been published by the FTC, or at least identified. It is difficult, many argue, for the regulated industry to glean rules of conduct from the published consent orders, and the FTC's repeated assertions that it is only demanding that companies employ "reasonable" security measures is singularly unhelpful when measured against a constantly evolving threat landscape.

Although the Wyndham ruling may embolden the FTC to continue its current case-by-case approach, challenges such as these are gaining support, and may nevertheless put more pressure on the FTC to issue specific security standards or at least point to existing voluntary best practices as models to follow.

In the midst of this debate is an open question whether the cybersecurity framework will influence the FTC's present strategy and provide a guidepost to evaluate data security. One the one side, some companies may voluntarily adopt the framework, which could be used as an external standard to manage risk and liability. On the other hand, the framework was developed to be voluntary and nonbinding, and the FTC's reliance on the framework could invite legal challenges.

Would Legislation Cure Ambiguity?

Regardless of how the pending lawsuits end, the FTC has also made it clear that it would like even more authority to regulate data security. Over the past few months, congressional committees held hearings examining the breaches at Target Corp. and Neiman Marcus Ltd. and possible policy responses that could be made. The hearings offered the first time for the FTC to comment on various congressional proposals to standardize data security and breach response.

Among the lines of questioning asked of the FTC in a February 2014 hearing before the House of Representatives, for example, was whether the FTC needs additional authority and how that authority should be constructed. In a telling "yes-no" colloquy with Rep. John Dingell, D-Mich., FTC Chairwoman Edith Ramirez provided some detail of what she would like to see in a legislative proposal.

When asked by the congressman about the scope of such a proposal, Chairwoman Ramirez said that it should cover all entities currently regulated by the FTC; there should be a federal standard administered by one agency — the FTC; if strong enough, it should preempt state laws; and violations of it should be seen as violations of the FTC Act. The momentum behind the cybersecurity framework may indicate support for such a federal standard, but it is unclear how states would respond or whether such a bill could pass Congress.

Conclusion

Although the FTC has sought to regulate data security under its existing Section 5 authority and through new legislation, the bounds of that authority remain murky despite the Wyndham decision. The FTC's assertive and aggressive push for authority has received the most attention, but the FTC is just one of many agencies trying to define its role in regulating data security, particularly in light of the president's Executive Order 13636, Improving Critical Infrastructure Cybersecurity, and the release of the cybersecurity framework. For example, the Department of Defense has started a rulemaking process and issued a report regarding cybersecurity regulations governing federal procurements.

Even if the cybersecurity framework provides some clarity regarding cybersecurity best practices, it is unclear what practical effect that document will have given that the framework developed in a different context (i.e., aligning critical infrastructure cybersecurity measures) and is intended to be completely voluntary. Indeed, the FTC may not want to back a standard with which it had limited involvement in developing.

In the absence of unambiguous authority vested with the FTC, other agencies will continue to jump on the data security bandwagon in the coming year, raising further questions regarding who is really in charge and which standards will apply. The ongoing challenges to the FTC's authority might end up affirming broad authority to regulate — and undercut the need for comprehensive legislation — or strip the FTC of its primary enforcement mechanism as challenges continue to evolve in judicial channels. Until then, data security will continue to be a significant issue for the FTC, and companies must be prepared to address the evolving compliance requirements despite ongoing regulatory uncertainty.

—By Christopher Cole, Elliot Golding and and Evan Wolff, Crowell & Moring LLP

Christopher Cole is a partner in Crowell & Moring's advertising and product risk management group in Washington, D.C. Elliot Golding is an associate and Evan Wolff is a partner in the firm's privacy and cybersecurity group in Washington.