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 Tips Data Security Hand In Wyndham Pact

By **Allison Grande**

Law360, New York (December 10, 2015, 10:21 PM ET) -- The Federal Trade Commission in its data security settlement with Wyndham endorsed a popular standard for securing payment card data and set out specific requirements for how to handle a franchisee breach, offering companies valuable insight into the perplexing issue of what the commission expects from them on the data security front, attorneys say.

Under the settlement filed in New Jersey federal court, which was disclosed by the parties Wednesday, Wyndham Worldwide Corp. subsidiary Wyndham Hotel and Resorts LLC agreed to establish a comprehensive information security program and undergo annual audits in order to resolve the commission's allegations that the hotel chain's lax data security practices unfairly exposed the payment card information of more than 600,000 consumers to hackers in three separate data breaches during a two-year period.

While the settlement shares many similarities with the more than 50 other data security consent decrees that the commission has reached with a range of businesses since 2001, the level of specificity when it comes to what standards Wyndham must follow to secure cardholder data and segregate its network from those of its franchisees helps shed some much-needed light on the long-simmering question of what the regulator considers to be "reasonable" data security under the unfairness prong of Section 5 of the FTC Act, attorneys say.

"The Wyndham settlement is really an evolution of the FTC's continued precedent in this area," ZwillGen PLLC counsel and chief information security officer Amy Mushahwar told Law360. "It offers some instructive insight into what the commission would do in the event of another significant payment card breach that involved several subsidiaries or franchisees."

In becoming the first company to challenge rather than settle an FTC data security case, Wyndham brought to the forefront a chorus of criticism vocalized by businesses who felt that the commission was using its unfairness authority without providing adequate notice of what exactly it considered "reasonable" data security practices to be.

Although the Wyndham pact doesn't totally crack the mystery, it does help to chip away at the lure for the wide range of companies swept up by the regulator's broad privacy enforcement net.

"Because the FTC has taken a case-by-case approach to enforcement, there is no complete list of things that companies can do to be guaranteed to escape FTC scrutiny," Harris Wiltshire & Grannis LLP attorney Adrienne Fowler said. "However, this consent decree is an important guide to what the FTC believes is reasonable."

As with the commission's previous data security deals, the pact announced Wednesday binds Wyndham for a 20-year term to the requirements of maintaining a comprehensive information security program and undergoing compliance audits on an annual basis.

But the settlement also included several details not included in prior data security settlements, including that the security program must specifically protect cardholder data, whereas previous deals mandated broader programs to safeguard a wide range of personally identifiable data.

"The proposed settlement in Wyndham is focused not just on an overall data security program but on specific safeguards directed at the payment card information, which was the point of the breach," said Craig A. Newman, a partner with Patterson Belknap Webb & Tyler LLP and chairman of the firm's privacy and data security practice. "The FTC's expectations going forward especially concerning the collection and storage of payment card information are pretty clear from the settlement."

The settlement also specifically calls out the Payment Card Industry Data Security Standard, or PCI DSS, that applies to all entities involved in payment processing as the benchmark for Wyndham to meet in its audits.

"By referring to that common industry standard, the FTC is essentially putting its stamp of approval on the standard and providing some assurance to the industry that to the extent that merchants comply with the widely applicable standard, that's likely providing reasonable security for payment card information," Fowler said.

Given that the PCI DSS specifies concrete steps that merchants must take to secure cardholder data rather than rely on abstract best practices followed by less-regulated industries, companies would be wise to ensure that their data security plans sync up with the standards, although attorneys were quick to caution that data security is not a one-size-fits-all proposition and that requirements don't should be tailored to the company rather than copied exactly.

"Companies that are dealing with PCI DSS are going to have to look at this case and this agreement and think about how it translates to their own security practices," Foley Hoag LLP attorney Christopher Hart said.

Aside from the payment card protections, the settlement also requires Wyndham to create effective barriers like firewalls between its corporate servers and those of its franchisees.

The provision was put into place to address the specific facts of the Wyndham breaches, which the FTC asserted occurred when hackers gained access to the network of a Wyndham franchisee and then exploited lax security on the hotel chain's corporate network to grab sensitive data from dozens of other Wyndham franchisees.

But the obligations imposed on Wyndham in regards to its franchisees' networks offer important insight into the commission's expectations regarding how companies deal with partners outside their own corporate networks, attorneys say.

"While that provision is tied to the underlying relationship Wyndham has with its franchisees, it brings to light a whole other layer of liability in a franchisor-franchisee relationship that many may not appreciate until now," said Fernando Pinguelo, the chairman of the cybersecurity and data protection group at Scarinci Hollenbeck LLC.

The parties' settlement came on the heels of a groundbreaking ruling issued by the Third Circuit in August, which held that the FTC has the power to regulate private companies' data security under the unfairness prong of Section 5 and that the hotel chain was not entitled to know with ascertainable certainty the commission's interpretation of what cybersecurity practices are required by the act.

"This sort of result was nearly inevitable once the Third Circuit issued its blistering ruling in August," said Montgomery McCracken Walker & Rhoads LLP partner Michael Hayes, who agreed that the settlement sets a "significant precedent" that the FTC should be expected to attempt to impose against a number of future enforcement targets.

Aside from establishing a potential framework for future resolutions, attorneys noted that the resolution was also significant because it shut down the possibility of any challenge to the Third Circuit's ruling, effectively cementing the FTC's power to bring enforcement actions inside and most likely outside the circuit.

"Until another circuit court weighs in, which is unlikely to happen in the foreseeable future, this Third Circuit ruling really becomes pretty persuasive authority for lower courts having to deal with the question of FTC authority in this area, which might make businesses think a little bit more about going into litigation in federal court," Hart said.

Settling the case also eliminated the possibility that a district court would for the first time weigh in on whether the commission’s data security allegations met the consumer harm threshold under Section 5(n) of the FTC Act.

Medical testing laboratory LabMD Inc. recently prevailed on these grounds in a data security proceeding brought by the FTC in an administrative court, with the commission's own chief administrative law judge concluding last month that the regulator had failed to prove that the lab’s alleged failure to institute reasonable data security had caused harm to consumers. The agency has appealed the ruling to its own commissioners.

“In credit card breaches, there are real issues about the extent of the consumer harm given both the legal limits on consumer liability and the zero liability policies of the major card brands,” said Kilpatrick Townsend & Stockton LLP big data, privacy and information security practice co-leader Jon Neiditz said, who noted that court records indicate that Wyndham signed the settlement documents released Wednesday several weeks before the LabMD decision was issued. “If Wyndham had continued, we would have found out how the FTC would try to prove its unfairness case under Section 5(n). But now, in the absence of something unexpected, the FTC is going to have to show that probability of consumer harm in the context of LabMD.”

Wyndham is represented by Justin T. Quinn of Robinson Miller LLC, Eugene F. Assaf and K. Winn Allen of Kirkland & Ellis LLP and Douglas H. Meal and David T. Cohen of Ropes & Gray LLP.

The FTC is represented in-house by Lisa Weintraub Schifferle, Kristin Krause Cohen, Kevin H. Moriarty,

Katherine E. McCarron, John A. Krebs, Jonathan E. Zimmerman, Andrea V. Arias, Allison M. Lefrak and James A. Trilling.

The case is Federal Trade Commission v. Wyndham Worldwide Corp. et al., case number 2:13-cv-01887, in the U.S. District Court for the District of New Jersey.

--Editing by Katherine Rautenberg and Christine Chun.