ROPES & GRAY

ALERT

Privacy & Data Security

December 22, 2015

Wyndham and FTC Agree to Consent Order Ending Data Security Breach Litigation

Attorneys
Douglas H. Meal
Heather Egan Sussman
James S. DeGraw
Seth C. Harrington
David McIntosh
Mark P. Szpak
Michelle Visser
Paul D. Rubin
Marc P. Berger
David T. Cohen

On Friday, December 11, 2015, the U.S. District Court for the District of New Jersey entered a consent order between the Federal Trade Commission ("FTC") and hospitality company Wyndham Hotels and Resorts, LLC ("Wyndham") along with several of its affiliates, putting to an end an FTC lawsuit alleging that Wyndham's data security practices violated Section 5 of the FTC Act. The *Wyndham* order is of interest to all companies that collect or receive payment card information and/or are subject to an FTC data breach investigation, not only because it ends the first ever fully contested FTC action over the application of Section 5 to data security, but also because it provides guidance on the FTC's position as to the elements of a reasonable data security program for payment card data. The *Wyndham* order is also notable for imposing narrower obligations on Wyndham than the FTC has typically obtained against the targets of its data security investigations.

The suit giving rise to the *Wyndham* order was brought by the FTC in 2012 in connection with three criminal network intrusions that may have compromised payment card information collected by several Wyndham-branded hotels. The FTC alleged that Wyndham and several of its affiliates committed "unfair" and "deceptive" practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, in connection with purported information security deficiencies at the Wyndham-branded hotels. Prior to this time, potential defendants in data security cases brought by the FTC had almost always entered into pre-litigation settlements with the agency, and the rare instances of litigation were merely brief precursors to entry of a consent order. In this case, however, Wyndham chose to aggressively defend against the FTC's allegations.

In 2014, the U.S. District Court for the District of New Jersey denied Wyndham's motion to dismiss the suit for failure to state a claim, but certified a portion of its ruling for appeal to the U.S. Court of Appeals for the Third Circuit. On appeal, the Third Circuit affirmed the denial of Wyndham's motion to dismiss, holding that the FTC has the power to regulate data security under the "unfair practices" prong of the FTC Act and that Wyndham had constitutionally sufficient notice that data security could fall within the ambit of the Act. The Third Circuit also suggested, however, that the FTC would have to meet a high burden of proof at trial – including, for the agency's "unfair practices" claim, proof of substantial, unavoidable consumer injury (beyond mere consumer inconvenience) that is not outweighed by countervailing benefits, and (potentially) proof that Wyndham acted deceptively or engaged in other misconduct beyond just having caused consumer injury of that sort.

Last month, in an FTC administrative proceeding against a lab testing company (LabMD), an FTC administrative law judge reinforced the Third Circuit's suggestion that the burden of proof for an unfairness claim is a demanding one in the data security context. Ruling on an unfairness-based claim brought by the FTC against LabMD over allegedly deficient data security practices, the judge held that FTC staff had failed to prove substantial consumer injury, and therefore ruled for LabMD on the merits. The FTC staff has appealed that decision to the FTC Commissioners.

It was against this backdrop that the FTC and Wyndham, along with the Wyndham affiliates that the FTC had included as defendants in its suit, agreed to the *Wyndham* order to terminate the FTC's lawsuit. The *Wyndham* order requires Wyndham to have in place a comprehensive information security program for payment card data Wyndham

collects or receives in the United States from or about consumers. Thus, in contrast to the FTC's typical data security order, the *Wyndham* order does *not* cover all personal information; instead, it covers only the type of personal information that the FTC alleged was put at risk in the cyberattacks that gave rise to its lawsuit, namely, payment card data. The distinction is significant, because companies like Wyndham that collect payment card data already are obliged by virtue of card brand rules to have in place a comprehensive information security program for payment card data, so this aspect of the order does not impose any additive obligation on such a company.

The order also requires Wyndham to obtain annual assessments as to whether it complies with specified data security standards for payment card data, and those assessments must include or be accompanied by the following certifications: the extent of Wyndham's compliance with the specified standards; whether Wyndham implements certain restrictions on unauthorized traffic coming into its network from Wyndham-branded hotels; the extent of Wyndham's compliance with a risk assessment protocol; and that the assessor is adequately qualified, uses accepted standards and is free from conflicts of interest. Here again, because large companies that collect payment card data already are required by virtue of card brand rules to undergo independent annual third-party assessments of their compliance with the applicable data security standards for payment card data, and because those assessments already encompass the company's compliance with the specified risk protocol, its protection of its network against unauthorized traffic emanating from external networks, and the assessor's qualifications, standards and freedom from conflicts of interest, these aspects of the order do not impose any additive obligations on such a company. The order also imposes limited reporting and record-keeping obligations.

The *Wyndham* order is also notable for not addressing several allegations the FTC included in its complaint. The FTC's complaint had alleged that Wyndham made deceptive statements about data security in its online privacy policy, but unlike other data security cases where the FTC has alleged deception the *Wyndham* order contains no restrictions on the statements Wyndham can make about data security. The FTC's complaint also sought to hold Wyndham responsible for the data security measures at independently owned Wyndham-branded hotels, but the *Wyndham* order places no such responsibility on Wyndham, and instead it merely requires that Wyndham take steps to protect Wyndham's *own network* against risks emanating from those hotels. The FTC's complaint alleged that not only Wyndham, but also one of its sister companies and two of its parent companies, were liable under Section 5 of the FTC Act. The *Wyndham* order imposes no obligations, however, on the sister company at all, and it merely requires the two parent companies to perform limited record-keeping and other administrative obligations and guarantee Wyndham's performance of the substantive obligations described above. The *Wyndham* order also does not include any monetary relief, even though the FTC's complaint requested it.

Finally, and perhaps most importantly, the *Wyndham* order is also the first FTC data security order to provide detailed compliance guidance. First, the *Wyndham* order states that the comprehensive information security program for payment card data shall consist of the following five enumerated requirements: designation of accountable employees, a risk assessment, use of reasonable safeguards, use of reasonable steps to retain certain service providers, and adjustment of the program over time. While these five requirements had been included in prior FTC data security orders, the *Wyndham* order is the first to clarify that these requirements are not merely necessary, but also sufficient, to satisfy the requirement to implement a comprehensive information security program.

Second, the *Wyndham* order is the first to include a safe harbor shielding the company from potential claims that it failed to implement the comprehensive information security program required by the order. Specifically, the *Wyndham* order provides that if Wyndham's annual assessment certifies that it fully complies with the specified data security standards, and also contains certain other required certifications, Wyndham will be deemed compliant with the requirement to maintain a comprehensive information security program for one year or until the next annual assessment deadline, whichever is earlier. This safe harbor is subject to two narrow qualifications. First, Wyndham will not obtain the safe harbor as to any company practice about which it made a representation to the assessor that misrepresented or omitted material information that would likely affect a reasonable assessor's evaluation, and if the misrepresentation or omission was made for the purpose of deceiving the assessor, Wyndham will not obtain a safe harbor as to any of its practices. Second, if Wyndham significantly changes a practice after an assessment, then in

order to maintain the safe harbor as to that practice, it must obtain a certification from an assessor that the change does not cause Wyndham to become non-compliant with the data security standards that were used in the assessment.

These two pieces of guidance amount, in effect, to statements by the FTC that compliance with the five enumerated security program requirements and/or the requirements for the safe harbor are sufficient to reasonably safeguard payment card information. For this reason, all companies that collect or receive payment card information may want to consider whether their practices comply with the five enumerated security program requirements and/or the requirements for the safe harbor.

Ropes & Gray represented Wyndham in the FTC lawsuit. For more information regarding the *Wyndham* order, or to discuss data security practices generally, please feel free to contact Doug Meal, who led the Ropes & Gray litigation team representing Wyndham, or Heather Sussman, Jim DeGraw, Seth Harrington, David McIntosh, Mark Szpak, Michelle Visser, Paul Rubin, Marc Berger, David Cohen, or another member of Ropes & Gray's leading privacy & data security team.