KING & SPALDING

Client Alert

Data, Privacy & Security Practice Group

December 11, 2015

The FTC's Proposed Wyndham Settlement and its Implications for the Regulatory Landscape

On December 9, 2015, the Federal Trade Commission (FTC), with the agreement of Wyndham Hotels and Resorts ("Wyndham"), filed a stipulated order for injunction ("Consent Order") in the U.S. District Court for the District of New Jersey to resolve the high-profile litigation concerning the hotel chain's protection of consumers' financial information. The Consent Order is expected to be entered by U.S. District Judge Esther Salas without much delay.

As we described in an earlier **Client Alert**, on August 24, 2015, the Third Circuit Court of Appeals issued a much-awaited decision in the case,[1] holding that the FTC has authority to regulate "unfair" or "deceptive" cybersecurity practices under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a). Wyndham's appeal was the most significant challenge to the FTC's cybersecurity authority to date, and the Third Circuit's decision, followed by a stipulated injunction against Wyndham, confirms the FTC's role as a leading cybersecurity regulator. With Wyndham's legal challenges behind it, the FTC may step up its enforcement activities, both independently and in collaboration with the Federal Communications Commission (FCC), which has recently emerged as another significant cybersecurity regulator.

Settlement Agreement Requires Wyndham to Establish Twenty-Year "Comprehensive Information Security Program" for Cardholder Data

The Consent Order does not impose a monetary penalty or require an admission of liability. Instead, the Consent Order imposes security requirements for the protection of "Cardholder Data," which generally refers to the full payment account number on a credit or debit card, and may also include the cardholder name and expiration date. The security requirements in the Consent Order are aligned with the Payment Card Industry Data Security Standard (also known as PCI DSS); as a result, the requirements may already be contractually imposed on Wyndham through major card brands such as Visa and MasterCard. In line with prior FTC settlements and consent orders, Wyndham must generally comply with the agreed-to terms for a period of twenty years. It also has a ten-year obligation to notify the

For more information, contact:

Norman J. Armstrong, Jr.
+1 202 626 8979
narmstrong@kslaw.com

Christopher C. Burris
+1 404 572 4708
cburris@kslaw.com

Nicholas A. Oldham
+1 202 626 3740
noldham@kslaw.com

Mark H. Francis
+1 212 556 2117
mfrancis@kslaw.com

Coleen P. Schoch
+1 404 572 2708
cschoch@kslaw.com

William S. McClintock
+1 404 572 3502
wmcclintock@kslaw.com

King & Spalding

Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600
Fax: +1 404 572 5100

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500
Fax: +1 202 626 3737

www.kslaw.com

FTC whenever it makes changes to the company's corporate structure or to the FTC's designated points of contact.

Wyndham has four significant obligations under the Consent Order:

> *Establish a "comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity" of Cardholder Data.*[2]

Under the Consent Order, Wyndham is required to (i) conduct an assessment that identifies "material internal and external risks" to the "security, confidentiality, and integrity" of Cardholder Data; (ii) implement and test safeguards that control the risks identified in the assessment; (iii) take reasonable steps to ensure that Wyndham's service providers safeguard Cardholder Data; and (iv) designate a Wyndham employee or employees who are accountable for the information security program. The program must comply with PCI DSS or another standard of comparable scope and thoroughness expressly approved by the FTC.

> *Undergo an annual audit of the company's Cardholder Data security practices.*[3]

The Consent Order requires Wyndham to engage an independent, third-party assessor to conduct an annual audit of the company's Cardholder Data security practices, and certify that Wyndham's practices comply with PCI DSS or a similar standard approved by the FTC. The assessor must also certify that Wyndham complies with a formal risk management and assessment protocol in accordance with the PCI DSS Risk Assessment Guidelines. Significantly, the assessor must assess Wyndham's relationship with its franchisees' Cardholder Data networks; in the annual audit, the assessor must certify whether franchisee networks are included in the annual corporate audit, whether they have independently been certified to comply with PCI DSS, or whether Wyndham treats them as "untrusted networks."

> *Obtain an independent assessment and incident report within 180 days of any data breach that involves more than 10,000 payment card numbers.*[4]

The Consent Order requires that Wyndham obtain independent assessments whenever there is a data breach or a significant change in the company's Cardholder Data security practices. Breach is described as an intrusion with reason to suspect the unauthorized disclosure, theft, modification, or destruction of Cardholder Data. Within 180 days of any breach that involves more than 10,000 payment card numbers, Wyndham must obtain a written assessment and incident report from an independent auditor. Card brands have similar requirements imposed on merchants through contractual relationships, namely, the retention of a Payment Card Industry Forensic Investigator (also known as a "PFI") to investigate and report on major breaches of Cardholder Data.

> *Receive an independent assessor's certification that any "significant change" to the company's information security practices complies with approved standards.*[5]

Whenever Wyndham institutes a "significant change" in any information security practice, it must obtain a certification from an independent assessor that the change does not cause Wyndham to fall out of compliance with the same standard that governs its annual audit. "Significant change" is left undefined in the Consent Order.

The FTC Lacks General Authority to Impose Fines for Cybersecurity Violations

The FTC has a very limited scope of authority to seek or impose monetary penalties for cybersecurity violations. In general, the FTC has authority to seek civil penalties for cybersecurity violations in three areas: (i) information collected online about minors that is subject to the Children's Online Privacy Protection Act (also known as "COPPA"); (ii) credit report information subject to the Fair Credit Reporting Act (also known as "FCRA"); and, (iii) violations of FTC administrative orders.[6]

The proposed *Wyndham* Consent Order reflects this limited authority to seek fines. The FTC sued Wyndham in U.S. District Court under Section 13(b) of the FTC Act, [7] which permits the FTC to seek and obtain permanent injunctions against violations of any law that the FTC enforces. These laws include the FTC's authority to regulate "unfair" or "deceptive" data practices under Section 5.[8] The Consent Order further illustrates how the FTC, even without the ability to impose fines, can still use its Section 13(b) power to seek and obtain injunctive relief that requires alleged cybersecurity violators to comply with significant, lengthy, and often costly compliance requirements. In fact, most companies pursued by the FTC for alleged Section 5 cybersecurity violations have agreed to administrative consent orders with a similar set of twenty-year obligations, presumably to avoid drawn out administrative actions or litigation in federal court.

Recent FTC Setback in LabMD Litigation

In addition to lacking a general authority to impose fines on violators, the FTC suffered a significant setback in another high-profile action on November 13, 2015, when Administrative Law Judge Michael Chappell dismissed the FTC's administrative complaint against LabMD.[9] Instead of filing a district court complaint (as it had in *Wyndham*), the FTC filed an administrative complaint against LabMD for cybersecurity violations.[10] The alleged violations were primarily based on a 1,718-page LabMD report that allegedly contained the personal information of 9,300 individual patients and was identified on an unsecure peer-to-peer file sharing network.[11] In his opinion dismissing the complaint, the ALJ held that the FTC failed to prove the necessary "actual or likely consumer harm" required to establish a Section 5 violation, because there was no evidence that LabMD's cybersecurity practices caused, or were likely to cause, actual consumer harm.[12] The FTC staff has announced that it intends to appeal the ALJ's decision to the full FTC Commission.[13] A decision by the Commission would be appealable to a federal court of appeals. Therefore, despite the Third Circuit's *Wyndham* decision that Section 5 of the FTC Act gives the Commission the authority to regulate "unfair" or "deceptive" cybersecurity practices,[14] *LabMD* raises some uncertainty regarding the FTC's practical ability to assert Section 5 violations regarding cybersecurity practices.

FTC Enforcement Contrasted with Recent FCC Enforcement Trends

The FCC has recently emerged as a robust actor in cybersecurity enforcement. In contrast to the FTC, the FCC asserts that it has a broad authority to impose large fines against cybersecurity violators. It has demonstrated recent success in translating this authority into large monetary settlements in this area. It has also hired personnel with significant experience in privacy and security, possibly indicating that it intends to continue to focus on this space.[15]

In October 2014, in its first case seeking fines for inadequate cybersecurity practices, the FCC proposed a $10 million fine against TerraCom Inc. and YourTel America Inc. for storing sensitive consumer data online in an unprotected, generally accessible location.[16] The parties later settled the dispute for $3.5 million in penalties.[17] In April 2015, the FCC obtained a $25 million penalty from AT&T for its failure to protect the CPNI—customer proprietary network

information—of nearly 280,000 AT&T customers.[18] In November 2015, in its first cybersecurity action against a cable operator, Cox Communications paid the FCC $595,000 to resolve an investigation into a hack that affected approximately 60 customers.[19]

There remains some dispute regarding the FCC's ability to impose fines for cybersecurity violations. The FCC has taken the position that it can seek forfeiture penalties for cybersecurity violations under Sections 222(a) and 503(b)(1) of the Communications Act.[20] However, a minority of FCC Commissioners have asserted that the Act does not give it the authority to regulate consumer cybersecurity.[21] Despite the lack of consensus, the FCC continues to seek and successfully obtain large monetary payments in cybersecurity settlements.

Given the agencies' different bases of statutory authority, the FTC will likely continue promulgating its view on reasonable cybersecurity practices by imposing long-term compliance programs on alleged violators, whereas the FCC appears inclined to encourage good practices by extracting significant penalties from telecommunications companies with allegedly insufficient protections on customer data.

November 2015 FTC-FCC Consumer Protection Memorandum of Understanding

Although the FTC and FCC have demonstrated different enforcement strategies, the two agencies recently announced their intention to cooperate on cybersecurity issues. In November, these agencies signed a Joint "FCC-FTC Consumer Protection Memorandum of Understanding."[22] Recognizing the FTC's "expertise and leadership on matters of consumer protection" and the FCC's "expertise and leadership with regard to consumer protection as applied to telecommunications services," the memorandum agrees that the agencies will: (i) collaborate and consult where initiatives or investigations will impact the other agency's authority or jurisdiction; (ii) share information, customer complaint data, and relevant expertise; and, (iii) "engage in joint enforcement actions" when their jurisdictions permit. Because the Memorandum of Understanding has been in effect for less than a month, it is unclear at this stage how it will alter the FTC's or the FCC's cybersecurity enforcement strategies, or how frequently the agencies' activities will overlap.

Conclusion

The proposed *Wyndham* settlement marks an end to the most significant litigation to date challenging the FTC's cybersecurity authority, although *LabMD* may bring further developments in the near future. The terms of the *Wyndham* settlement cement the FTC's role as a leading data privacy and security enforcer, despite its limited authority to seek monetary penalties from violators. The FCC's willingness to seek fines for cybersecurity violations in the telecommunications sector, its recent hires, and its planned collaboration with the FTC, all demonstrate an intent to increase its participation in this regulatory environment. Businesses should be mindful of the evolving legal landscape as federal and state regulators increasingly issue guidance and pursue investigations in regard to corporate cybersecurity practices.

King & Spalding's Data, Privacy, and Security Practice

King & Spalding is particularly well equipped to assist clients in the area of privacy and information security law. Our **Data, Privacy & Security Practice** regularly advises clients regarding the myriad statutory and regulatory requirements that businesses face when handling personal customer information and other sensitive information in the U.S. and globally. This often involves assisting clients in developing comprehensive privacy and data security programs, responding to data security breaches, complying with breach notification laws, avoiding potential litigation arising out of internal and external data security breaches, defending litigation, whether class actions brought by those affected by data breaches, third party suits, or government actions, and handling both state and federal government investigations and enforcement actions.

With more than 50 Data, Privacy & Security lawyers in offices across the United States, Europe and the Middle East, King & Spalding is able to provide substantive expertise and collaborative support to clients across a wide spectrum of industries and jurisdictions facing privacy and data security-based legal concerns. We apply a multidisciplinary approach to such issues, bringing together attorneys with backgrounds in corporate governance and transactions, healthcare, intellectual property rights, complex civil litigation, e-discovery, government investigations, government advocacy, insurance recovery, and public policy.

If you have any questions about the Wyndham settlement or related issues, please contact **Norman Armstrong Jr.** at +1 202 626 8979, **Christopher C. Burris** at +1 404 572 4708, **Nicholas A. Oldham** at +1 202 626 3740, **Mark H. Francis** at +1 212 556 2117, **Coleen P. Schoch** at +1 404 572 2708, or **William S. McClintock** at +1 404 572 3502.

---

[1] *Fed. Trade Comm'n v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).
[2] Stipulated Order for Injunction at 4-6, *Fed. Trade Comm'n v. Wyndham Worldwide Corp.*, No. 2:13-cv-1887 (D.N.J. Dec. 9, 2015), ECF No. 282-1.
[3] *Id.* at 6-8.
[4] *Id.* at 8.
[5] *Id.* at 9.
[6] *See, e.g.*, 15 U.S.C. § 45; *see also* Jessica Rich, Director of the Fed. Trade Comm'n, Bureau of Consumer Protection, Prepared Statement to the House Subcommittee on Commerce, Manufacturing, and Trade ,Mar. 18, 2014, at 11, *available at* https://www.ftc.gov/system/files/documents/public_statements/630961/150318datasecurity.pdf (last visited Dec. 11, 2015).
[7] Complaint at 2, *Fed. Trade Comm'n v. Wyndham Worldwide Corp*., No. 2:13-cv-1887 (D.N.J. Dec. 9, 2015), ECF No. 1.
[8] 15 U.S.C. § 53(b).
[9] Initial Decision, *In re LabMD, Inc.*, No. 9357 (F.T.C. Nov. 13, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/151113labmd_decision.pdf.
[10] Complaint, *In re LabMD, Inc.*, No. 9357 (F.T.C. Aug. 28, 2015), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2013/08/130829labmdpart3.pdf.
[11] Initial Decision at 22-25, *In re LabMD, Inc.*, No. 9357 (F.T.C. Nov. 13, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/151113labmd_decision.pdf.
[12] *Id.* at 51.
[13] Complaint Counsel's Notice of Appeal, *In re LabMD, Inc.*, No. 9357 (F.T.C. Nov. 24, 2015), *available at* https://www.ftc.gov/system/files/documents/cases/580032_-_labmd_-_complaint_counsels_notice_of_appeal.pdf.

[14] For a more detailed analysis of the *Wyndham* litigation and the Third Circuit's decision, see Norman Armstrong *et al.*, *Federal Appeals Court Recognizes for the First Time the FTC's Authority to Enforce Cybersecurity Practices*, Aug. 28, 2015, *available at* http://www.kslaw.com/imageserver/KSPublic/library/publication/ca082815.pdf.
[15] Andrea Peterson and Brian Fung, *With this hire, the FCC could get tougher on privacy and security*, WASHINGTON POST, Nov. 24, 2015, https://www.washingtonpost.com/news/the-switch/wp/2015/11/24/with-this-hire-the-fcc-could-soon-get-tougher-on-privacy-and-security/ (last visited Dec. 11, 2015) (announcing the hire of prominent privacy practitioner Jonathan Mayer as the FCC's "technical lead for investigations into telephone, television, and Internet service providers").
[16] John C. Richter *et al.*, "New Sheriff in Town: FCC Expands Its Reach to Data Security," Privacy & Sec. L. Rep. (BNA) No. 13, at 2042 (Dec. 8, 2014), *available at* http://www.kslaw.com/imageserver/KSPublic/library/publication/2014articles/12_8_14_BNA.pdf.
[17] *Id.*; Allison Grande, *FCC's Cox Fine Shows Minor Hacks Can Have Major Fallout*, Law360, Nov. 12, 2015, *available at* http://www.law360.com/articles/725691/fcc-s-cox-fine-shows-minor-hacks-can-have-major-fallout (last visited Dec. 11, 2015).
[18] Fed. Commc'ns Comm'n, *AT&T to Pay $25 Million to Settle Consumer Privacy Investigation: FCC's Largest Data Security Enforcement Action*, Apr. 8, 2015, *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-332911A1.pdf .
[19] *See supra* note 17.
[20] *See supra* note 16.
[21] See *id.*
[22] FCC-FTC Consumer Protection Memorandum of Understanding, Nov. 16, 2015, *available at* https://www.ftc.gov/system/files/documents/cooperation_agreements/151116ftcfcc-mou.pdf.