KING & SPALDING

Client Alert

Data, Privacy & Security Practice Group

August 28, 2015

Federal Appeals Court Recognizes for the First Time the FTC's Authority to Enforce Cybersecurity Practices

On August 24, 2015, the Third Circuit Court of Appeals issued a much-awaited decision in *FTC v. Wyndham Worldwide Corporation*,[1] holding that the Federal Trade Commission (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). The decision may not only enhance the FTC's authority going forward, it could also inspire other federal and state agencies acting under similar statutory language to forge ahead with enforcement of cybersecurity practices. We thus recommend that companies: (i) institute comprehensive cybersecurity governance programs; and (ii) utilize the National Institute of Standards and Technology's ***Framework for Improving Critical Infrastructure Cybersecurity*** ("Framework") or another comprehensive model to maintain practices that will be articulable and defensible in the ever-evolving legal landscape.

The FTC's Authority to Regulate Cybersecurity

The FTC is the federal agency charged with, among other things, protecting consumers from unfair and deceptive trade practices. The FTC's enforcement authority is derived from over 70 different statutes, including the Federal Trade Commission Act.[2] Section 5 of the Federal Trade Commission Act ("Section 5") authorizes the FTC to bring actions—in both judicial and administrative forum—against entities engaging in "unfair or deceptive acts or practices in or affecting commerce." More specifically, an act or practice is unlawful if it (i) is likely to cause substantial injury; (ii) is not outweighed by countervailing benefits to consumers and competition; and (iii) could not reasonably have been avoided by consumers.[3]

The FTC has interpreted its Section 5 authority as allowing it to regulate—and to bring enforcement actions related to—allegedly unfair or deceptive acts or practices in the cybersecurity arena. The FTC has also issued guidance on cybersecurity topics, including the protection of consumer privacy, physical security, and cybersecurity involving connected devices (*i.e.,* "the internet of things").

For more information, contact:

Norman 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

James L. Michaels
+1 404 572 2809
jmichaels@kslaw.com

King & Spalding

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

New York
1185 Avenue of the Americas
New York, NY 10036
Tel: +1 212 556 2100
Fax: +1 212 556 2222

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

Unlike other government agencies that are only beginning to flex their cybersecurity enforcement muscles, the FTC has been pursuing companies for allegedly deficient cybersecurity programs for nearly twenty years. As a result, the FTC has been a leading federal regulatory authority on cybersecurity and privacy, and has brought over 50 cases since 2002 against companies allegedly engaged in unfair or deceptive practices that put consumers' personal data at unreasonable risk.[4]

In one of the earliest and most influential cases, the FTC alleged in 2002 that several Microsoft products made under its "Passport" brand, including one intended for children, did not live up to the promises made in their privacy policies. The FTC and Microsoft entered into a settlement whereby Microsoft agreed to implement a written cybersecurity program and allow the FTC to oversee that implementation. Importantly, there was no indication that any personal data was actually taken due to problems with Passport's cybersecurity mechanisms, but the FTC initiated action against Microsoft nonetheless.[5] Two years later, in 2004, the FTC and Petco settled allegations that Petco.com did not take appropriate measures to defend against cyberattacks, despite express claims that consumer data used on that site (including credit card numbers) would remain secure. In that case, consumer data was actually compromised by a malicious hacker who used a SQL injection attack to steal data. The settlement required Petco to cease from making false representations about the strength of its cybersecurity program and to establish a new, more secure cybersecurity program.[6]

The FTC remains active in the cybersecurity sphere, continuing to bring complaints against companies that allegedly do not take necessary steps to safeguard consumer data. In just the past two years, the FTC has settled a number of cybersecurity cases through consent decrees, including a case where a company allegedly tried to obtain health information from medical vendors without appropriate authorization from patients,[7] a case where a laptop containing personal information was allegedly stolen,[8] and a case where a company allegedly verified that websites were secure without actually confirming that those websites complied with security requirements.[9]

Yet for all its efforts in enforcing corporate cybersecurity practices, the FTC has declined to promulgate rules or explicitly identify a particular set of required cybersecurity measures or practices. Instead, the FTC contends that its view on the reasonableness of a cybersecurity program can be extrapolated from industry guidance, the FTC's reports and website publications,[10] and FTC enforcement actions.[11]

FTC v. Wyndham Worldwide Corp.

In 2012, the FTC filed a complaint alleging serious cybersecurity lapses at global hospitality company Wyndham Worldwide Corporation. According to the FTC's complaint, Wyndham's failure to maintain an effective cybersecurity program led to substantial consumer injury, and Wyndham's privacy policy misrepresented the cybersecurity measures in place at the company. Between 2008 and 2010, Wyndham was hacked three times, and personal information from over 600,000 Wyndham customers was taken by hackers in Russia. This data included credit card information, the taking of which allegedly resulted in fraudulent use of those cards to the tune of $10.6 million.

Wyndham moved to dismiss the FTC's suit on the grounds that the FTC lacked the authority to regulate cybersecurity under Section 5 of the Federal Trade Commission Act and that, even if the FTC had the authority to regulate cybersecurity, it had not put companies on notice—by publishing rules and regulation—of what constituted an adequate cybersecurity program. The district court rejected both of these arguments and Wyndham appealed to the Third Circuit. As mentioned above, the Third Circuit affirmed the district court's decision on August 24, 2015, which

was the first time an appellate court ruled on the FTC's interpretation of its Section 5 authority in the cybersecurity arena.

The Third Circuit discussed the various deficiencies with Wyndham's cybersecurity program and then held that the FTC had the authority to bring suit because Wyndham's conduct did not fall outside of the plain meaning of "unfair." Wyndham's alleged cybersecurity deficiencies included (i) storing payment card information in clear, readable text; (ii) using default passwords; (iii) failing to use firewalls; (iv) not restricting Wyndham network access by third party vendors; (v) not employing reasonable measures to prevent unauthorized access to Wyndham computers; and (vi) publishing a privacy policy that overstated its level of cybersecurity. The Third Circuit also rejected Wyndham's argument that it did not have fair notice of what specific cybersecurity practices the FTC believes are necessary. In reaching this conclusion, the Third Circuit found especially convincing the fact that the FTC had alleged that Wyndham's cybersecurity measures were grossly deficient:

> [T]he complaint does not allege that Wyndham used *weak* firewalls, IP address restrictions, encryption software, and passwords. Rather, it alleges that Wyndham failed to use *any* firewall at critical network points, did not restrict specific IP addresses *at all*, did not use *any* encryption for certain customer files, and did not require some users to change their default or factory-setting passwords *at all.*[12]

The Third Circuit also found significant that Wyndham had been hacked three times: "certainly after the second time Wyndham was hacked, it was on notice of the possibility that a court *could* find that its practices fail the cost-benefit analysis" conducted in determining whether it had fair notice.[13]

The Third Circuit's holding that the FTC's established practice of regulating cybersecurity is supported by its statutory mandate is hardly a surprise in the context of increasing scrutiny being given to cybersecurity by several regulatory agencies. Especially noteworthy is the fact that the Third Circuit likely could have reached this conclusion even absent Wyndham's allegedly misleading statements in its privacy policy, implying that it is likely that the cybersecurity lapses standing alone would be the proper subject of an FTC enforcement action.

The Next Battleground for the FTC

With resolution of the FTC's Section 5 authority over cybersecurity in the Third Circuit, attention may shift to the Eleventh Circuit, where the FTC's battle with LabMD is being played out. In 2013, the FTC issued an Administrative Complaint against LabMD alleging that it may have engaged in "unfair . . . acts or practices" in regard to cybersecurity protecting healthcare information. LabMD filed two consecutive lawsuits against the FTC to enjoin the administrative proceedings,[14] twice appealing to the Eleventh Circuit,[15] and arguing that the FTC has no statutory authority to address its cybersecurity practices under Section 5. The Eleventh Circuit has held that it lacks jurisdiction to address the merits of the case in the absence of final agency action.[16] The administrative proceedings are currently in the midst of post-trial briefing, after which there may be a final showdown at the Eleventh Circuit.

A Broader Context: Government Oversight Beyond the FTC

As a whole, federal agencies are increasingly interested in the cybersecurity practices of organizations within their respective jurisdiction, although they have taken different approaches in their initial steps. Some agencies, like the Food and Drug Administration and Department of Energy, have issued guidance and attempted to raise awareness of best practices.[17] The SEC has issued rules for registered broker- dealers, investment companies, and investment

advisors subject to its authority, and even sent formal inquiries to a number of organizations touching on their cybersecurity posture.[18]

Beyond the organizations directly under its authority, the SEC has broad authority to ensure transparency and full disclosure in the securities marketplace, and it has wielded that power to require securities issuers to disclose any cybersecurity-related risks or events that a reasonable investor would consider material to an investment decision. To that end, the staff of the SEC's Division of Corporation Finance issued guidance in 2011 to help issuers determine whether they needed to disclose certain cyber-vulnerabilities, past cyber-attacks, and other cybersecurity matters.[19] The primary adverse consequences discussed in the 2011 Guidance include remediation costs, increased cybersecurity costs, lost revenues, litigation, and reputational damage.[20] The 2011 Guidance notes that, "as with other operational and financial risks, registrants should review, on an ongoing basis, the adequacy of their disclosure relating to cybersecurity risks and cyber incidents."[21] Registrants are, therefore, encouraged to consider the probability of cyber incidents and the "quantitative and qualitative magnitude of those risks."[22]

Furthermore, 47 of the 50 U.S. states have enacted breach notification statutes that are triggered when an organization experiences a cyber incident. Some states have also passed laws requiring organizations to adopt "reasonable" cybersecurity practices for particularly sensitive PII, such as social security numbers, without providing specific guidelines for achieving such reasonableness.[23] In addition to pursuing violations of state breach notification laws, state attorneys general also pursue enforcement under consumer protection acts—most commonly in the form of Unfair and Deceptive Trade Practice Acts ("UDTPAs"). Unlike narrower breach notification laws, state UDTPAs are often modeled after the broad language in Section 5(a) of the Federal Trade Commission Act, and state authorities can interpret their states' "unfair" and "deceptive" provisions to address cybersecurity practices.

Recommendation

As demonstrated in the *Wyndham* decision, companies should view cybersecurity as a primary legal risk. Ultimately, the *Wyndham* decision recognizes that the statutory requirement is determined by 15 U.S.C. § 45(n), which asks whether "the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." The Court held that "this standard informs parties that the relevant inquiry here is a cost-benefit analysis," and underscores how the **NIST Framework** is an ideal model for addressing legal obligations. The Framework is a risk-based model and can therefore be employed to measure (and document) the expected costs and benefits inherent in every cybersecurity practice. In addition, the NIST Framework is the only model developed at the express direction of an Executive Order from a U.S. President,[24] it has been championed by numerous federal agencies, and is frequently cited by members of Congress.

* * *

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

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 cybersecurity-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. Our **Data, Privacy & Security Practice** has unparalleled experience in areas ranging from providing regulatory compliance advice, to responding to security incidents including data breaches and cybersecurity incidents, interfacing with stakeholders and the government, engaging in complex civil litigation (such as class actions), handling state and federal government investigations and enforcement actions, and advocating on behalf of our clients before the highest levels of state and federal government.

If you have any questions about the *Wyndham* decision 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, or **James L. Michaels** at +1 404 572 2809.

---

[1] *FTC v. Wyndham Worldwide Corp*., No. 14-3514 (3d Cir. Aug 24, 2015) (Ambro, J.).
[2] 15 U.S.C. §§ 41-58.
[3] 15 U.S.C. § 45(n); *see generally In the Matter of CardSystems Solutions, Inc. et al.,* FTC Dkt. No. C-4168 (Sept. 5, 2006) (complaint); *In the Matter of DSW, Inc.*, FTC Dkt. No. C-4157 (Mar. 7, 2006) (complaint); *United States v. ChoicePoint, Inc*., No. 106-cv-0198, Dkt. No. 5 (N.D. Ga. Feb. 15, 2006) (stipulated judgment); *In the Matter of BJ's Wholesale Club, Inc*., FTC Dkt. No. C-4148 (Sept. 20, 2005) (complaint).
[4] *See* Federal Trade Commission 2014 Privacy and Data Security Update, https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf.
[5] *See* FTC Press Release, *Microsoft Settles FTC Charges Alleging False Security and Privacy Promises* (Aug. 8, 2002), available at https://www.ftc.gov/news-events/press-releases/2002/08/microsoft-settles-ftc-charges-alleging-false-security-privacy.
[6] *See* FTC Press Release, *Petco Settles FTC Charges* (Nov. 17, 2004), available at https://www.ftc.gov/news-events/press-releases/2004/11/petco-settles-ftc-charges.
[7] *In the Matter of PaymentsMD, LLC*, FTC Dkt. No. C-4505 (Jan. 5, 2015).
[8] *See* FTC Press Release, *Accretive Health Settles FTC Charges That It Failed to Adequately Protect Consumers' Personal Information* (Dec. 31, 2013), available at https://www.ftc.gov/news-events/press-releases/2013/12/accretive-health-settles-ftc-charges-it-failed-adequately-protect.
[9] *See* FTC Press Release, *TRUSTe Settles FTC Charges it Deceived Consumers Through Its Privacy Seal Program* (Nov. 17, 2014), available at https://www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its.
[10] The FTC has a webpage dedicated to this subject at https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security.
[11] *See FTC v. Wyndham Worldwide Corp*., 10 F. Supp. 3d 602, 616-17 (D.N.J. 2014) (noting the FTC's position that "in the data-security context, 'reasonableness is the touchstone,' . . . 'unreasonable data security practices are unfair,' . . . [and reasonableness] can be enforced in an industry-specific, case-by-case manner").
[12] *FTC v. Wyndham Worldwide Corp*., --- F.3d ----, 2015 WL 4998121 at *14 (3rd Cir. August 24, 2015) (internal citations omitted; emphasis in original).
[13] *Id.* (emphasis in original).
[14] *See LabMD v. FTC*, No. 1:13-cv-1787 (D.D.C.); *LabMD v. FTC*, No. 1:14-cv-00810 (N.D. Ga).
[15] *See LabMD Inc. v. FTC*, No. 13-15267-F (11th Cir. Feb. 18, 2014); *LabMD Inc. v. FTC*, 776 F.3d 1275 (11th Cir. 2015).
[16] *LabMD Inc.*, 776 F.3d at 1280.
[17] *See, e.g.,* Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, FDA (Oct. 2, 2014) (FDA guidance to medical device manufacturers recommending adoption of the NIST Framework); Energy Sector Cybersecurity Framework Implementation Guidance, DOE (Jan. 2015), http://energy.gov/oe/downloads/energy-sector-cybersecurity-framework-implementation-guidance.
[18] Rule 30 of the SEC's Regulation S-P requires these entities to "adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information." 17 C.F.R. § 248.30. In April 2014, the SEC's Office of Compliance Inspections and Examinations ("OCIE") announced plans to examine the cybersecurity practices of

broker-dealers and investment advisors, and published a detailed list of sample questions it would be issuing. OCIE Cybersecurity Initiative (Apr. 15, 2014), http://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf.

[19] *See* SEC Division of Corporation Finance, CF Disclosure Guidance: Topic No. 2 (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm. This is the only formal guidance provided by the SEC to date on this topic.

[20] *Id*.

[21] *Id*.

[22] *Id*. (emphasis added); *see also Basic v. Levinson*, 485 U.S. 224 (1988) ("Information is considered material if there is a substantial likelihood that a reasonable investor would consider it important in making an investment decision or if the information would significantly alter the total mix of information available").

[23] *See, e.g.,* Connecticut General Statutes 743dd.

[24] *See* 78 Fed. Reg. 11739, Executive Order 13636, Improving Critical Infrastructure Cybersecurity (Feb. 19, 2013).