The Federal Trade Commission's Enforcement of Data Security Standards

by Ryan T. Bergsieker, Richard H. Cunningham, and Lindsey Young

The Federal Trade Commission is positioning itself to be the primary federal regulator of data security practices. This article overviews the legal standards the Commission has applied to assess companies' data security practices and suggests steps companies can take to minimize their exposure to an FTC enforcement action in the event of a data breach.

Seemingly every week a front page headline reports a cyber attack involving the theft of the personal or financial information of millions of consumers. Although companies that have suffered a data breach are victims of a crime, regulators and plaintiffs' attorneys may seek to hold such companies liable for "failing to lock the door" to adequately protect the stolen data.

This article provides an overview of the active and ongoing efforts by the Federal Trade Commission (Commission or FTC) to hold companies responsible for sufficiently securing sensitive consumer data. While multiple government agencies conduct regulatory investigations of companies' data security practices,[1] the FTC increasingly is positioning itself as the primary federal data security regulator. The article also describes the FTC's legal authority for regulating data security practices, which is currently being tested for the first time, and the legal standards the FTC applies when considering data security issues. It concludes by noting steps organizations can take to reduce their exposure to a potential FTC enforcement action should they suffer a data breach.

The FTC's Asserted Enforcement Authority

Congress established the FTC as an independent agency in 1914.[2] The FTC's primary mission is to promote consumer protection and eliminate and prevent anticompetitive business practices.[3] The agency is led by a chairperson and four additional commissioners, each of whom is nominated by the President and confirmed by the Senate for a seven-year term.[4] One political party cannot hold more than three commissioner seats at any given time.[5]

Section 5(a) of the FTC Act (§ 5) empowers the FTC to "prevent persons, partnerships, or corporations . . . from using . . . unfair or deceptive acts or practices in or affecting commerce."[6] Congress added § 5(n) in 1994 to specify that conduct is "unfair" only if it "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 competition."[7]

This statutory language is quite general and in no way references data security or liability for data breaches. Notwithstanding its

Coordinating Editors

Katherine M.L. Pratt, Boulder, of Berg Hill Greenleaf & Ruscitti LLP—(303) 402-1600, kmlp@bhgrlaw.com; Todd Seelman, Denver, of Lewis Brisbois Bisgaard & Smith LLP—(720) 292-2002, todd.seelman@lewisbrisbois.com

About the Authors

Ryan T. Bergsieker is Of Counsel in the Denver office of Gibson, Dunn & Crutcher LLP. A former federal computer crimes prosecutor, his practice focuses on complex civil litigation, white-collar criminal and regulatory defense, and information security/data privacy counseling. Richard H. Cunningham is also Of Counsel at Gibson, Dunn & Crutcher LLP in Denver. His practice focuses on consumer protection and antitrust matters, including counseling, government investigations, and litigation. Before joining Gibson Dunn, Rich served as Senior Trial Counsel at the Federal Trade Commission's Bureau of Competition. Lindsey Young is an associate in the Palo Alto office of Gibson, Dunn & Crutcher LLP. She currently practices in the firm's Litigation Department. Before joining Gibson Dunn, she worked in consumer behavior and media research.



Antitrust and Consumer Protection Law articles are sponsored by the Antitrust and Consumer Protection Subsection of the CBA Business Law Section to provide information about and explain the complexities of antitrust and consumer protection laws.

non-specific statutory authority, in 2002 the FTC began asserting that insufficient data security practices—whether or not they lead to a breach—can be unfair and/or deceptive and thus violate § 5.[8] Over the last thirteen years, the FTC has asserted data security violations against more than fifty companies that have elected to settle the agency's allegations.[9] The FTC refers to its settlements as "consent orders."

Challenges to the FTC's Authority to Regulate Data Security Practices

Two recent FTC targets, Wyndham Worldwide and LabMD, have elected to contest the FTC's allegations in enforcement actions brought in federal court and administrative litigation, respectively. Indeed, as outlined below, Wyndham and LabMD have raised broad challenges to the FTC's authority to regulate data security practices.[10]

Wyndham Worldwide

In June 2012, the FTC filed suit in the U.S. District Court for the District of New Jersey against Wyndham Worldwide, a global hotel company.[11] The complaint stemmed from discovery that intruders had obtained unauthorized access to Wyndham's computer networks on three separate occasions between 2008 and 2010, once via a "brute force attack" that involved guessing users' passwords, and twice via access to an administrator account on Wyndham's network.[12] Taken together, the breaches compromised more than 619,000 consumer payment card numbers and led to more than $10.6 million in fraudulent charges.[13] The FTC alleged that Wyndham violated the unfairness prong of § 5 by "fail[ing] to employ reasonable and appropriate measures to protect personal information against unauthorized access."[14] The FTC further alleged that Wyndham violated the deceptiveness prong of § 5 by representing to consumers that it employed reasonable and appropriate security measures when in fact it had not.[15]

Wyndham moved to dismiss the complaint, challenging the FTC's authority to regulate data security practices on two grounds, both of which were rejected by the court.[16] First, Wyndham argued that the passage by Congress of various laws that touch on data security,[17] including the Gramm-Leach-Bliley Act and the Children's Online Privacy Protection Act, limits the FTC's § 5 authority over data security issues.[18] The court disagreed, holding that "the FTC's unfairness authority over data security can coexist with the existing data-security regulatory scheme."[19] Second, Wyndham asserted that due process requires the FTC to promulgate regulations before bringing unfairness enforcement claims.[20] The court again disagreed, finding that the test under § 5(n) added by Congress in 1994, as well as past FTC complaints and consent orders, provide sufficient notice of what is prohibited.[21] The court's order is currently the subject of an interlocutory appeal before the Third Circuit. Following oral arguments and the submission of supplemental briefing in March 2015, the Third Circuit is likely to issue a decision later this year.[22]

LabMD

In August 2013, a few months after Wyndham filed its motion to dismiss in the District of New Jersey, the FTC opted for a different forum when it sued LabMD, a clinical lab testing company, alleging that LabMD violated § 5(a) of the FTC Act's prohibition against unfair acts or practices by failing to "develop, implement, or maintain a comprehensive information security program" to protect consumers' sensitive personal and health information.[23] The complaint arose from two separate security incidents. In one of the incidents, a LabMD report containing the names, birth dates, social security numbers, and insurance policy numbers of 9,300 consumers was found on a peer-to-peer file sharing application. In the second incident, police found copied checks and sheets including the names and Social Security numbers of several hundred consumers who had interacted with LabMD in possession of individuals who pleaded no contest to identity theft charges.[24] The FTC brought the suit in its administrative capacity before an FTC Administrative Law Judge (ALJ) rather than in a district court.[25]

Like Wyndham, LabMD moved to dismiss the complaint on the ground that the FTC lacks authority to regulate data security practices because there is nothing in § 5 explicitly authorizing the FTC to regulate such practices.[26] The Commission—which has the authority to resolve such motions filed in connection with administrative proceedings—disagreed, finding that Congress had delegated "broad authority . . . to determine what practices were unfair, rather than enumerating the particular practices to which [the term 'unfair'] was intended to apply."[27] LabMD further argued that the FTC may not adjudicate specific conduct as violating § 5 without first promulgating regulations or legislative rules that put companies on notice of what does or does not violate the law.[28] The Commission also rejected this argument, stating that "such complex questions relating to data security practices in an online environment are particularly well-suited to case-by-case development in administrative adjudications or enforcement proceedings."[29]

Before the Commission denied LabMD's motion to dismiss, LabMD filed a motion to stay the administrative proceedings in the Eleventh Circuit. The Eleventh Circuit *sua sponte* dismissed the motion for lack of jurisdiction.[30] Then, in March 2014, after receiving the Commission's ruling, LabMD filed a motion for preliminary injunction in the Northern District of Georgia to enjoin the FTC's administrative proceeding.[31] The FTC moved to dismiss the case for lack of jurisdiction and failure to state a claim, and the district court granted this motion on jurisdictional grounds in May 2014,[32] a decision LabMD immediately appealed to the Eleventh Circuit.[33] The Eleventh Circuit affirmed the district court's decision on January 20, 2015.[34] Meanwhile, the FTC's administrative suit against LabMD has continued to move forward, and is on track to be decided by the ALJ in 2015. After the Commission reviews the ALJ decision, it will issue a final opinion. If the FTC or LabMD elects to pursue appellate review, the Eleventh Circuit will review the merits of the Commission's decision and whether the Commission has jurisdiction to adjudicate data security issues in the first place.

The pending litigation regarding the FTC's authority in *Wyndham* and *LabMD* has not inhibited the vigor with which the FTC is pursuing data security issues. The agency pursued eight data-security-related enforcement actions in 2014, all of which resulted in consent orders, as the *Wyndham* and *LabMD* jurisdictional challenges have moved through the courts. The agency has also continued to conduct investigations of data security issues, some of which have been disclosed in securities filings by the targets of those investigations, and numerous others that remain non-public.

FTC Standard for Evaluating Data Security Protocols

The FTC applies a reasonableness test to determine whether a company's data security practices are unfair and/or deceptive; that is, the Commission asks whether a company's practices are

> reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities.[35]

The Commission has issued several pieces of guidance to inform companies regarding its view of reasonable data security practices. In addition, the Commission's fifty-plus enforcement actions and settlements provide additional context against which to assess whether companies' data security practices are reasonable. In practice, these myriad sources of less-than-definitive authority make it challenging, especially for counsel unfamiliar with practice before the Commission, to counsel clients regarding exactly where the Commission draws the line between reasonable and unreasonable data security practices.

In 2009, the FTC published a data security "Guide for Business" that contains checklists for companies to gauge how their practices measure up across five key principles of data security ("Take Stock; Scale Down; Lock It; Pitch It; Plan Ahead").[36] The Guide for Business contains almost eighty recommended practices, but does not specify which, if any, are necessary or sufficient to comply with the FTC's view of what constitutes adequate data security standards. In addition, many of the suggestions are very general, such as recommendations to "train employees to recognize security threats" and "[h]ave a plan in place to respond to security incidents."[37]

Earlier this year, the Commission issued guidance relating to the "Internet of Things," which refers to everyday objects that send and receive data via the Internet, such as fitness bracelets and smart thermostats.[38] In the report, the FTC emphasized that companies should adopt reasonable limits on the collection and retention of consumer data, especially when such data is collected for business purposes unrelated to operation of the device itself.[39] As with its recommendation to scale down the collection and retention of data in its Guide for Business,[40] the FTC's focus on data minimization further signals that failure to properly reduce data collection and retention may become increasingly relevant to the FTC's analysis of reasonableness under § 5.

The FTC's complaints[41] and consent orders provide some additional clarity regarding the dividing line between data security practices that do and do not violate § 5. There are some rules of the road[42] that can be distilled from the Commission's guidance and prosecutorial record:

1. Companies cannot misrepresent (or describe in a misleading way) their processes and practices for securing sensitive consumer information.[43]
2. Companies need to respond quickly and reasonably to identified vulnerabilities. For example, companies should consider retaining outside experts to address problems that exceed internal capabilities.[44]
3. Companies should limit access (for example, with passwords and firewalls) to sensitive information and employ other widely used tools to address risks that are known within the company or industry.[45]
4. When companies maintain sensitive information, they must train employees to protect that information.[46]
5. Companies should require vendors with access to sensitive information to implement data security protocols, and monitor their compliance.[47]
6. Companies must encrypt sensitive data, absent a legitimate reason not to do so.[48]
7. More rigorous (and expensive) protections are required of larger organizations possessing large volumes of sensitive information.[49]

These general propositions are easy to list but often difficult to implement in practice. Placing sensitive consumer data, such as credit card or social security numbers, on a database that is accessible to anyone over the Internet is clearly a practice that will invite § 5 scrutiny from the FTC and is easy to avoid in most instances, but what else constitutes a commonly known risk? What form of encryption is sufficient?[50] If a vulnerability is identified, what steps

must a company take to remediate that risk? How quickly must it do so? The FTC declines to answer these questions by taking the position that "there is no one-size-fits-all data security program."[51] However, the FTC does stop well short of taking the position that any breach is dispositive evidence of insufficient data security practices.[52]

Notably, several FTC enforcement actions are premised on the target failing to follow up on risks identified in the usual course of business or by consultants. Thus, in effect, whatever standard was applied internally or by the consultants becomes the Commission's *de facto* standard for reasonable security practices. While this approach may offer simplicity from an investigative perspective, it provides an incentive to organizations to avoid frank self-assessment; punishes organizations with exacting, no-stone-unturned approaches to risk assessment; and lacks substantive objectivity or consistency.

Strategies to Minimize the Risk of an FTC Enforcement Action

In addition to following the rules of the road noted above, legal counsel should encourage companies to take a number of steps before a breach has occurred to minimize the likelihood that the FTC will, on conducting a post-breach investigation, view the company's data security practices as deceptive or unfair under § 5. These steps are discussed below.

➢ **Implement a data security program.** This should involve regular employee training, physical asset management, data encryption, access controls, secure destruction, and data loss prevention mechanisms. Employee training is particularly critical, because many data breaches involve an element of social engineering—for example, an e-mail with a link containing malware that enables attackers to access a corporate system.

➢ **Develop and maintain a data breach response plan.** The plan should identify a cross-disciplinary internal response team (for example, IT engineers, in-house/outside attorneys, communications specialists, and operations personnel) and include current contact information for those individuals, and draft retention agreements for all necessary outside personnel. The plan should also include a clear delegation of authority and escalation procedures, as well as a post-incident feedback loop to improve response capabilities. Among the reasons to maintain a data breach response plan is that it ensures that in the fast-paced moments after initial discovery of a potential data breach, privilege is maintained, where appropriate, over the post-breach investigation. Another reason is to ensure that the company considers whether and how to make proper notifications, after conferring with counsel, to the company's key constituencies, including insurance carriers.

➢ **Ensure that cybersecurity is a focus of the executive team and board of directors.** This is not just the responsibility of the IT department. Companies that in good faith have made cybersecurity an organizational priority are, on balance, more likely to be able to persuade the FTC that they truly are victims, not culprits, following a data breach. Leaders at the highest levels of the organization should focus on what data the company maintains and the form in which the company maintains that data, to help ensure both proper data minimization and the implementation of adequate security standards. These leaders also should focus on asking whether lessons learned from any previous breaches or audits have been translated into process improvements.

➢ **Verify that the IT department monitors potential security risks and has a reasonable escalation process for any identified issue.** Because the standards the FTC applies to determine whether a company has taken reasonable precautions with consumers' data are fluid, documents showing that the company had actual knowledge of weaknesses in its systems and failed to follow up on them are often subjects of discussion in post-breach regulatory inquiries. Documents showing that a company did not move forward with IT improvements because of budget constraints are also frequently subjects of such discussions.

➢ **Walk through data breach scenarios and mock responses to such scenarios.** For example, consider how to handle employee theft, a stolen laptop, and a hacking incident.

In the moments following the discovery of a data breach, these preparations can help make the difference between a coordinated, thorough, and timely response, and a disjointed, damaging, delayed effort. Responding to a data breach in a coordinated way is critical to successfully navigating any follow-up FTC investigation for at least two reasons. First, doing so demonstrates to the FTC that the company is on top of the data breach and is responding in a way that is likely to ensure that harm to consumers from this breach and the likelihood of future breaches are minimized. Second, as noted above, maintaining control of the investigation increases the likelihood that privilege can be maintained, where appropriate, lessening the likelihood that poorly phrased documents sent out in a non-privileged form during a fast-paced breach investigation will later be misconstrued when requested by the FTC.

Conclusion

Data security enforcement is a relatively new phenomenon, with the FTC making an aggressive bid to establish liability and remedial standards that apply across all sectors of the economy. While it is possible that the *Wyndham* and *LabMD* cases will lead to some modification of the FTC's approach in this area, it is unlikely that the FTC will abandon regulation of data security practices entirely, whatever the outcome of those cases. Thus, familiarity with the FTC's views on data security and its investigative practices can allow companies to significantly reduce their exposure to FTC enforcement actions in the event of a breach, now and into the future.

Notes

1. Apart from the FTC, other U.S. regulators active in the data security area include state attorneys general, the Securities and Exchange Commission, the Department of Defense, the Department of Energy, and the Federal Communications Commission. In addition, multiple foreign jurisdictions—including the European Union, the United Kingdom, France, Germany, and Canada—have their own data security regulations and requirements. Moreover, virtually every U.S. state has enacted breach notification statutes that require companies to give consumers notice of a data breach in specified circumstances that vary by state.

2. FTC Act, 15 USC §§ 41 to 58 (2012).

3. FTC, "What We Do," www.ftc.gov/about-ftc/what-we-do.

4. 15 USC § 41.

5. *Id.*

6. 15 USC § 45(a)(2).

7. 15 USC § 45(n).

8. FTC Commissioner Julie Brill, "On the Front Lines: The FTC's Role in Data Security," Keynote Address Before the Center for Strategic and International Studies (Sept. 17, 2014).

9. FTC, "Commission Statement Marking the FTC's 50th Data Security Settlement" (Jan. 31, 2014).

10. *See* Motion to Dismiss, *FTC v. Wyndham Worldwide, Corp.*, No. 2:13-cv-01887-ES-SCM (D.N.J. April 26, 2013); Motion to Dismiss, *In the Matter of LabMD, Inc.*, FTC Docket No. 9357 (Nov. 12, 2013).

11. Complaint, *FTC v. Wyndham Worldwide Corp.*, No. CV 12-1365-PHXPGR (D.N.J. June 26, 2012) (amended Aug. 9, 2012).

12. *Id.* at ¶¶ 26-39.

13. *Id.* at ¶ 40.

14. *Id.* at ¶¶ 47-49.

15. *Id.* at ¶¶ 44-46.

16. *FTC v. Wyndham Worldwide Corp.*, 10 F.Supp.3d 602 (D.N.J. 2014).

17. *See* Fair Credit Reporting Act, 15 USC §§ 1661 *et seq.*; Gramm-Leach-Bliley Act, 15 USC §§ 6801 to 09; Children's Online Privacy Protection Act, 15 USC §§ 6501 to 06; Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

18. Motion to Dismiss, *Wyndham Worldwide*, No. 2:13-cv-01887-ES-SCM at *7-14 (analogizing to *Brown & Williamson*, which held that the FDA did not have jurisdiction over tobacco regulation due to more recent, tobacco-specific legislation).

19. *Wyndham*, 10 F.Supp.3d at 613.

20. Motion to Dismiss, *Wyndham Worldwide*, No. 2:13-cv-01887-ES-SCM at *14-18.

21. *Wyndham*, 10 F.Supp.3d at 619.

22. FTC Brief on Interlocutory Appeal, *FTC v. Wyndham Hotels & Resorts, LLC*, No. 2:13-cv-01887-ES-JAD (3d Cir. Nov. 5, 2014) (No. 14-3514).

23. *In the Matter of LabMD, Inc.*, FTC Docket No. 9357, Complaint at ¶¶ 22-23 (Aug. 28, 2013).

24. *Id.* at ¶¶ 17-21.

25. The FTC may pursue alleged § 5 violations either in federal court pursuant to § 13(b) or in its administrative capacity under § 5(b). The processes differ in numerous respects, but the most significant differences are that the FTC cannot obtain monetary relief in an administrative proceeding (without further proceedings in a federal district court under § 19), and the FTC has stated its preference to litigate novel issues in its administrative court. *See generally* 15 USC §§ 45(b) and 53(b).

26. *LabMD, Inc.*, FTC Docket No. 9357, Motion to Dismiss at *20 (Nov. 12, 2013).

27. *LabMD, Inc.*, FTC Docket No. 9357, Order Denying Motion to Dismiss at *4 (Jan. 16, 2014) (internal citation omitted).

28. *LabMD, Inc.*, FTC Docket No. 9357, Motion to Dismiss at *24-30 (Nov. 12, 2013) (arguing, among other things, that "the Internet postings of 'Guides for Business' . . . do not replace Federal Register publication" in providing the required notice).

29. *LabMD, Inc.*, FTC Docket No. 9357, Order Denying Motion to Dismiss at *14 (Jan. 16, 2014).

30. *LabMD, Inc. v. FTC*, No. 13-15267-F, 2014 U.S. App. LEXIS 9802 (11th Cir. Feb. 18, 2014).

31. Motion for Preliminary Injunction, *LabMD, Inc. v. FTC*, No. 1:14-cv-00810-WSD, 2014 U.S. Dist. LEXIS 65090 (N.D.Ga. March 20, 2014).

32. *LabMD, Inc. v. FTC*, No. 1:14-cv-00810-WSD, 2014 U.S. Dist. LEXIS 65090 at *23 (N.D.Ga. May 12, 2014).

33. Notice of Appeal, *LabMD, Inc. v. FTC*, No. 14-12144-EE (11th Cir. May 14, 2014).

34. *LabMD, Inc. v. FTC*, 776 F.3d 1275, 1280 (11th Cir. 2015).

35. FTC, "Commission Statement Marking the FTC's 50th Data Security Settlement" (Jan. 31, 2014).

36. FTC, "Protecting Personal Information: A Guide for Business" (Nov. 2011), www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf.

37. *Id.* at 19, 23.

38. FTC, "Internet of Things: Privacy & Security in a Connected World" (Jan. 2015), www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

39. *Id.* at 33-37.

40. FTC, *supra* note 36.

41. The FTC discloses a complaint when it settles cases pursuant to consent orders.

42. The Commission's complaints rarely, if ever, state that a particular act or practice is universally unlawful; rather, the FTC alleges that a company's practices "taken together" fail to provide "reasonable and appropriate" security protections.

43. *See, e.g., In the Matter of Credit Karma, Inc.*, FTC Docket No. C-4480, Complaint at ¶¶ 5-6 (Aug. 13, 2014); *In the Matter of Snapchat, Inc.*, FTC Docket No. C-4501, Complaint at ¶¶ 6-9 (Dec. 23, 2014). Notably, eight of the nine enforcement actions in which the FTC has obtained monetary relief have included misrepresentations to consumers about the company's security practices.

44. *See, e.g., In the Matter of Fandango, LLC*, FTC Docket No. C-4481, Complaint at ¶ 4 (Aug. 13, 2014); *In the Matter of Ceridian Corp.*, FTC Docket No. C-4325, Complaint at ¶ 2 (June 8, 2011).

45. *See, e.g., In the Matter of The TJX Companies, Inc.*, FTC Docket No. C-4227, Complaint at ¶ 2 (July 29, 2008); *In the Matter of Twitter, Inc.*, FTC Docket No. C-4316, Complaint at ¶ 4 (March 2, 2011).

46. *See, e.g., In the Matter of Franklin's Budget Car Sales, Inc.*, FTC Docket No. C-4371, Complaint at ¶ 2 (Oct. 3, 2012); *In the Matter of James B. Nutter Corp.*, FTC Docket No. C-4258, Complaint at ¶ 2 (June 12, 2009).

47. *See, e.g., In the Matter of CBR Systems, Inc.*, FTC Docket No. C-4400, Complaint at ¶ 2 (April 29, 2013); *In the Matter of Genelink, Inc.*, FTC Docket No. C-4456, Complaint at ¶ 13 (May 8, 2014).

48. *See, e.g.,* FTC, Closing letter to Verizon Communications, Inc. (Nov. 12, 2014) (asserting that use of old encryption methods is not sufficient), www.ftc.gov/enforcement/cases-proceedings/closing-letters/verizon-communications-inc; *In the Matter of Upromise, Inc.*, FTC Docket No. C-4351, Complaint at ¶ 5 (March 27, 2012); *In the Matter of Compete, Inc.*, FTC Docket No. C-4384, Complaint at ¶ 5 (Feb. 20, 2013).

49. FTC, "Commission Statement Marking the FTC's 50th Data Security Settlement" (Jan. 31, 2014) (highlighting that the reasonableness of a company's practices depends on the "volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities").

50. *See* FTC, Closing letter to Verizon, *supra* note 48 (asserting that use of old encryption methods is not sufficient), www.ftc.gov/system/files/documents/closing_letters/verizon-communications-inc./141112verizonclosingletter.pdf.

51. FTC, *supra* note 49.

52. *Id.* (stating that the FTC "does not require perfect security"). ■