Congressional Research Service
Informing the legislative debate since 1914

The Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices (UDAP) Authority

(name redacted)
Legislative Attorney

September 11, 2014

Congressional Research Service
7-....
www.crs.gov
R43723

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

The Federal Trade Commission Act established the Federal Trade Commission (FTC or Commission) in 1914. The protection of consumers from anticompetitive, deceptive, or unfair business practices is at the core of the FTC's mission. As part of that mission, the FTC has been at the forefront of the federal government's efforts to protect sensitive consumer information from data breaches and regulate cybersecurity. As the number of data breaches has soared, so too have FTC investigations into lax data security practices. The FTC has not been delegated specific authority to regulate data security. Rather, the FTC has broad authority under Section 5 of the Federal Trade Commission Act (FTC Act) to prohibit unfair and deceptive acts or practices.

In 1995, the FTC first became involved with consumer privacy issues. Initially, the FTC promoted industry self-regulation as the preferred approach to combatting threats to consumer privacy. After assessing its effectiveness, however, the FTC reported to Congress that self-regulation was not working. Thereupon, the FTC began taking legal action under Section 5 of the FTC Act. Section 5 of the FTC Act prohibits unfair or deceptive acts or practices. Since 2002, the FTC has pursued numerous investigations under Section 5 of the FTC Act against companies for failures to abide by stated privacy policies or engage in reasonable data security practices. It has monitored compliance with consent orders issued to companies for such failures. Using the deception prong of its statute, the FTC has settled more than 30 matters challenging companies' claims about the security they provide for consumers' personal data and more than 20 cases alleging that a company's failure to reasonably safeguard consumer data was an unfair practice. Because most of the FTC's privacy and data security cases were resolved with settlements or abandoned, there have been few judicial decisions. Against this backdrop, there are now two pending cases testing the FTC's unfairness authority under Section 5 of FTC Act as a means to respond to data breaches. These cases could have far-reaching implications for the liability of companies whose computer systems suffer a data breach. Both cases are the subject of a great deal of interest from Congress, businesses, trade groups, corporate law firms, and legal scholars.

In April 2014, in *FTC v. Wyndham Worldwide Corp.*, a federal district court denied a motion to dismiss, thereby effectively lending support to the FTC's position that it possesses jurisdiction to regulate data security practices under its authority to bring enforcement actions against unfair or deceptive practices. In another case, *In the Matter of LabMD*—an administrative enforcement action brought against a medical diagnostics laboratory—the commission rejected a motion to dismiss that challenged the FTC's authority to impose sanctions under the FTC Act. Both decisions are currently being appealed. *Wyndham* is on appeal to the Third Circuit, and LabMD has asked the Eleventh Circuit for the third time to intervene. The FTC's administrative action against LabMD was stayed this summer pending a related congressional hearing.

Several cyber and data security bills before Congress include provisions that would explicitly authorize the FTC to issue rules to implement data security standards and assess civil penalties. The FTC has called for federal legislation that would strengthen its existing authority governing data security standards and require companies to provide breach notification to consumers. This report provides background on the FTC and its legal authorities in the context of data security, and discusses the two aforementioned cases.

Contents

Contacts

The Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices (UDAP) Authority

The Federal Trade Commission Act (FTC Act) established the Federal Trade Commission (FTC or Commission) in 1914.[1] Its creation was prompted by efforts to "bust the trusts," which were late 19th century monopolistic corporations that frequently engaged in unethical commercial practices and stifled competition. The protection of consumers from anticompetitive, deceptive, or unfair business practices is at the core of the FTC's mission. As part of that mission, the FTC[2] has been at the forefront of the federal government's efforts to protect sensitive consumer information from data breaches, and to regulate cybersecurity. Data breaches occur when there is a loss or theft of, or other unauthorized access to, sensitive personally identifiable information (PII) that could result in the potential compromise of the confidentiality or integrity of data.[3] As the number of data breaches continues to soar,[4] so too do the number of FTC investigations[5] into lax data security.[6]

Data breaches have become almost ubiquitous in every sector of the economy. Businesses, financial and insurance services, retailers and merchants, educational institutions, government and military agencies, healthcare entities, and non-profit organizations have suffered cyber intrusions into their computer networks. Cybercriminals have targeted the payment systems of several of the nation's largest retailers in order to obtain credit and debit card information to conduct fraudulent transactions. In the last year alone, large scale hacks were disclosed by Target, Neiman Marcus, Michaels, and Home Depot.

Since 2002, the FTC has investigated the data security practices of many companies, and brought enforcement actions against 50 companies that have engaged in "unfair or deceptive" practices

[1] Sept. 26, 1914, ch. 311, 38 Stat. 717, 15 U.S.C. §§41 *et seq.*

[2] United States Government Manual, *Federal Trade Commission, available at* http://www.usgovernmentmanual.gov/Agency.aspx?EntityId=COjTKcMuGi4=&ParentEId=+klubNxgV0o=&EType=jY3M4CTKVHY=&S=aRQlxBKxNBs=.

[3] CRS Report R42475, *Data Security Breach Notification Laws*, by (name redacted). *See,* Grande, Allison, *FTC Steps Up Privacy Enforcement, With No Slowdown In Sight*, Law360 (July 23, 2014).

[4] Symantec's 2013 Internet Security Threat Report cites 253 data breaches which exposed over 552 million sets of personal data in 2013. Symantec Corp., *2014 Internet Security Threat Report* (Apr. 2014), *available at* http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.

[5] *See, e.g.,* Dave & Buster's, Inc., No. C-4291 (F.T.C. May 20, 2010) (consent order), available at http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2010/06/dave-busters-incin-matter; DSW, Inc., No. C-4157 (F.T.C. Mar. 7, 2006) (consent order), available at http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2006/03/dsw-incin-matter; BJ's Wholesale Club, Inc., No. C-4148 (F.T.C. Sept. 20, 2005) (consent order), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2005/09/bjs-wholesale-club-inc-matter; The TJX Cos., Inc., No. C-4227 (F.T.C. July 29, 2008) (consent order), *available at* http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2008/08/tjx-companies-inc-matter.

[6] Comm. on Nat'l Security Sys., National Information Assurance (IA) Glossary 21 (Instruction No. 4009 (June 2006)), available at http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf.

that put consumers' personal data at unreasonable risk in violation of the FTC Act. Section 5 of the FTC Act prohibits unfair or deceptive acts or practices.[7]

The FTC's authority to regulate data security under Section 5 of FTC Act is being challenged in two pending cases. In *FTC v. Wyndham Worldwide Corp.*,[8] a federal district court judge denied a motion to dismiss, thereby effectively lending support to the FTC's position that it possesses jurisdiction to regulate data security under its unfair or deceptive practices authority. In another data security case, *In the Matter of LabMD,*[9] the commission rejected a motion to dismiss in an administrative enforcement action brought against a medical diagnostics laboratory. Both decisions are currently being appealed. The *Wyndham* district court granted the hotel chain's motion for immediate appeal of the ruling to the U.S. Court of Appeals for the Third Circuit (Third Circuit) to consider the commission's authority to bring data security cases.[10] The FTC's administrative action against LabMD was stayed by the commission pending a congressional hearing investigating the firm, Triversa, a key player in the FTC's case.[11] Separately, LabMD has asked the U.S. Court of Appeals for the Eleventh Circuit (Eleventh Circuit) for the third time to dismiss the administrative action.[12]

Both cases are the subject of a great deal of interest from Congress, businesses, trade groups, corporate law firms, and legal scholars. Outside of government, there has been an academic debate over the scope of the FTC's authority respecting data security. Some scholars have argued that specific legislation is needed to give the FTC express authority to take action, under well-defined regulations against companies that experience data security breaches.[13] Other information privacy law scholars counter that the "FTC enforcement has certainly changed over the course of the past fifteen years, but the trajectory of development has followed a predictable set of patterns. These patterns are those of common law development."[14] This report will discuss the FTC's legal authority under Section 5 of the FTC Act in relation to data security, and the two aforementioned cases.

---

[7] 15 U.S.C. §45(a). Fed. Trade Comm'n, Bureau of Consumer Protection, *Privacy & Data Security Update* 3(June 2014), *available at* http://www.ftc.gov/reports/privacy-data-security-update-2014. ("An overview of the FTC's enforcement, policy initiatives, and consumer outreach and business guidance in the areas of privacy and data security, from January 2013-March 2014.").

[8] *FTC v. Wyndham Worldwide Corp.,* Civil Action No. 13-1887 (ES) (D.N.J. Apr. 7, 2014).

[9] *LabMD, Inc.*, Docket No. 9357, 2014 FTC LEXIS 2; 2014-1 Trade Cas. (CCH) P78,784, (Jan. 16, 2014).

[10] *FTC v. Wyndham Worldwide Corp*., Civil Action No. 13-1887 (ES) (D.N.J. June 23, 2014), 2014 U.S. Dist. LEXIS 84914; 2014-1 Trade Cas. (CCH) P78,817.

[11] The Federal Trade Commission and Its Section 5 Authority: Prosecutor, Judge, and Jury: Hearing Before the H. Comm. on Oversight and Gov't Reform, 113th Cong. (2014), http://oversight.house.gov/hearing/federal-trade-commission-section-5-authority-prosecutor-judge-jury-2/.

[12] Andrew Scurria, "*LabMD Makes 3rd Appellate Bid To Stop FTC Data Case,"* Law360 (June 25, 2014), *available at* http://www.law360.com/articles/551755/labmd-makes-3rd-appellate-bid-to-stop-ftc-data-case.

[13] Michael D. Scott, *The FTC, the Unfairness Doctrine and Data Security Litigation: Has the Commission Gone Too Far?* 60 Admin. L. Rev. 127 (2008).

[14] Daniel J. Solove, and Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 Colum. L. Rev. 583 (2014). See also, The Federal Trade Commission and Its Section 5 Authority: Prosecutor, Judge, and Jury: Hearing Before the H. Comm. on Oversight and Gov't Reform, 113th Cong. (2014) (statement of Woodrow Hartzog, Associate Professor of Law), http://oversight.house.gov/wp-content/uploads/2014/07/Hartzog-Statement-7-24-FTC.pdf.

Background

The FTC first became involved with consumer privacy issues in 1995.[15] Initially, the FTC promoted industry self-regulation as the preferred approach to protecting consumer privacy. After assessing its effectiveness, however, the FTC reported to Congress that self-regulation was not working.[16] Thereupon, the FTC began taking legal action against entities that violated their own privacy policies, asserting that such actions constituted "deceptive trade practices" under Section 5(a) of the FTC Act which prohibits unfair or deceptive acts or practices.[17] The FTC acknowledged that, although it had the power under Section 5 of the FTC Act to pursue deceptive practices, such as a website's failure to abide by a stated privacy policy, the agency could not require companies to adopt privacy policies.[18] To remedy this, the FTC proposed legislation[19] that would provide it with the authority to issue and enforce specific privacy regulations.[20]

In 2001, a change in presidential administrations and in FTC leadership caused the agency to shift its priorities from seeking new privacy legislation to expanding enforcement of consumer protection laws in order to target companies that had inadequate data security practices. The FTC's new focus resulted in the filing of numerous investigations, based on its Section 5 unfairness authority[21] against companies that experienced data security breaches resulting in a loss or theft of, or other unauthorized access to, sensitive personal information.[22] In general, the FTC's most recent unfair practices complaints allege that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information caused, or was likely to cause, substantial injury to consumers; that consumers cannot reasonably avoid such injury; and the company's failure in this regard is not outweighed by countervailing benefits to consumers or competition. Such failures are alleged to be in violation of Section 5 of the FTC Act.[23]

---

[15] Internet Privacy Hearing: Before the H. Subcomm. on Courts and Intellectual Property of the H. Judiciary Comm. 2 (March 26, 1998) (statement of David Medine, Associate Director for Credit Practices, Bureau of Consumer Protection, Federal Trade Commission), http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-internet-privacy/privacy.pdf.

[16] Fed. Trade Comm'n, Privacy Online: A Report to Congress (June 1998), http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

[17] 15 U.S.C. §45(a) states:

> Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.

[18] Fed. Trade Comm'n, *Privacy Online: A Report to Congress* (June 1998), a*vailable at* http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

[19] Fed. Trade Comm'n, *Privacy Online: A Report to Congress* (June 1998), a*vailable at* http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf. For information on the FTC's early privacy enforcement actions, see CRS Report RS21221, *Privacy Protection for Online Information*, by (name redacted).

[20] CRS Report R41756, *Privacy Protections for Personal Information Online*, by (name redacted).

[21] Fed. Trade Comm'n, *FTC Policy Statement on Unfairness* (Dec. 17, 1980), *available at* http://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

[22] Michael D. Scott, *The FTC, the Unfairness Doctrine and Data Security Litigation: Has the Commission Gone Too Far?* 60 Admin. L. Rev. 127 (2008). ("The Commission has held no hearings, solicited no public comments, engaged in no rulemaking, nor issued any policy statements or guidelines on when, if ever, the unfairness doctrine can, or should, be applied to data security breaches. Instead, the agency merely began filing complaints against companies that suffered such breaches.").

[23] *See*, *e.g., FTC v. Wyndham Worldwide Corp*., Civil Action No. 12-1365 (PGR) (D. Ariz. Aug. 9, 2012)(Compl. ¶ 47-49) (The complaint was originally filed in Arizona and transferred to the New Jersey court), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/08/120809wyndhamcmpt.pdf.

In March 2012, the FTC issued a Privacy Report[24] which articulated "best practices" for companies collecting and using data that can be reasonably linked to a consumer, computer, or device. Entities that collect only non-sensitive data from fewer than 5,000 consumers per year and that do not share the data with third parties would not have to adhere to the practices.

In 2014, in tandem with the announcement of its fiftieth settlement in a data security case, the FTC issued a statement outlining, among other things, its approach to data security:

> The touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be 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. Through its settlements, testimony, and public statements, the Commission has made clear that it does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks; there is no one-size-fits-all data security program; and the mere fact that a breach occurred does not mean that a company has violated the law.[25]

In addition, the commission provides educational materials to industry and the public about what "reasonable" data security generally entails. The FTC's approach to reasonable data security is based on broad principles. According to the FTC, the basic principles of a reasonable data security program are that companies should (1) know what consumer information they have and what employees or third parties have access to it; (2) limit the information they collect and retain based on their legitimate business needs; (3) protect the information they maintain by assessing risks and implementing protections in certain key areas—physical security, electronic security, employee training, and oversight of service providers; (4) properly dispose of information that they no longer need; and (5) have a plan in place to respond to security incidents, should they occur.[26]

Section 5 of the Federal Trade Commission Act

The FTC has not been delegated explicit authority to regulate data security. Rather, the FTC has broad authority under Section 5 of the Federal Trade Commission Act to prohibit "unfair or deceptive acts or practices in or affecting commerce.... "[27] Under Section 5 of the FTC Act, an act or practice is unfair if the act or practice (1) "causes or is likely to cause substantial injury to consumers," (2) "which is not reasonably avoidable by consumers themselves," and (3) "not outweighed by countervailing benefits to consumers or to competition."[28]

---

[24] Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change* (March 2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[25] Fed. Trade Comm'n, Commission Statement Marking the FTC's 50th Data Security Settlement (January 31, 2014), http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf.

[26] *See* Fed. Trade Comm'n, *Protecting Personal Information: A Guide for Business* (Nov. 2011), available at http://business.ftc.gov/documents/bus69-protecting-personal-information-guide-business. *See generally* Federal Trade Commission, Bureau of Consumer Protection Business Center, *Data Security Guidance*. *Available at* http://business.ftc.gov/privacy-and-security/data-security.

[27] 15 U.S.C. §45(n).

[28] 15 U.S.C. §45(n) states:

> The Commission shall have no authority under this section or section 57a of this title to declare

(continued...)

Indeed, it is widely acknowledged that "[t]he Commission and the Federal courts have been applying these three "unfairness" factors for decades and, on that basis, have found a wide range of acts or practices that satisfy the applicable criteria to be "unfair," even though—like the data security practices alleged in this case—"there is nothing in Section 5 explicitly authorizing the FTC to directly regulate" such practices."[29]

Congress chose not to enumerate the types of acts or practices that would constitute unfairness. As explained in the conference report accompanying the FTC Act's passage in 1914,

> It is impossible to frame definitions which embrace all unfair practices. There is no limit to human inventiveness in this field. Even if all known unfair practices were specifically defined and prohibited, it would be at once necessary to begin over again. If Congress were to adopt the method of definition, it would undertake an endless task.[30]

Failure to protect consumers' personal information is considered by the FTC to be an unfair or deceptive act or practice.[31]

Investigations

The FTC is generally authorized by the FTC Act to "gather and compile information concerning, and to investigate from time to time the organization, business, conduct, practices, and management of any person, partnership, or corporation engaged in or whose business affects commerce.... "[32] The FTC conducts data security investigations on a case-by-case basis to examine whether a company has "reasonable and appropriate security measures" to protect consumers' personal information. Following an investigation, the commission may initiate an enforcement action through administrative or judicial processes if it has "reason to believe" that the law is being or has been violated.[33] The FTC Act authorizes the FTC to seek injunctive and other equitable relief, including consumer redress, for violations.[34] The FTC does not possess

(...continued)

> unlawful an act or practice on the grounds that such act or practice is unfair unless 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. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.

[29] *In the Matter of LabMD, Inc.*, 2014 FTC LEXIS 2; 2014-1 Trade Cas. (CCH) P78,784, (F.T.C. Jan. 16, 2014).

[30] See H.R. Conf. Rep. No.1142, 63rd Cong., 2d Sess. 19 (1914).

[31] Fed. Trade Comm'n, *Division of Privacy and Identity Protection*. ("The Division of Privacy and Identity Protection, the newest of the Bureau's divisions, oversees issues related to consumer privacy, credit reporting, identity theft, and information security..... Specifically the Division enforces: Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices, including deceptive statements and unfair practices involving the use or protection of consumers' personal information; ..."); *available at* http://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions/division-privacy-and-identity.

[32] 15 U.S.C. §46(a) (excepted are banks, savings and loan institutions ... Federal credit unions ... and common carriers.... "), *see also* U.S. Federal Trade Commission, *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, available at http://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

[33] 15 U.S.C. §45(b).

[34] *Id.*

explicit authority to issue civil penalties for data security violations of the FTC Act[35] and is limited to fining companies for violating a settlement order.[36] Fines issued by the FTC must reflect the amount of consumer loss. If the respondent elects to settle the charges, it may sign a consent agreement (without admitting liability), consent to entry of a final order, and waive all right to judicial review. If the FTC accepts such a proposed consent agreement, it places the order on the record for public comment. If the respondent contests the charges, an Administrative Law Judge (ALJ) issues an "initial decision" recommending either entry of an order to cease and desist or dismissal of the complaint. Either party, or both, may appeal the initial decision to the full FTC. The respondent may file a petition for review of the full FTC decision with any court of appeals. If the court of appeals affirms the commission's order, it enters an order of enforcement. The losing party may seek Supreme Court review.[37]

The FTC also enforces several other statutes that impose obligations upon businesses to protect consumer data.[38] The FTC's Safeguards Rule implements the Gramm-Leach-Bliley Act's (GLBA)[39] data security requirements for non-bank financial institutions.[40] The Fair Credit Reporting Act (FCRA)[41] requires consumer reporting agencies to use reasonable procedures to ensure that the entities that disclose sensitive consumer information have a permissible purpose for receiving that information. The Children's Online Privacy Protection Act (COPPA)[42] requires website operators and online services to maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children. The FTC also oversees the EU-U.S. Safe Harbor Agreement.[43]

Enforcement Actions

Since 2002, under its unfair and deceptive practices authority, the FTC has brought and settled 50 data security enforcement actions against companies for failure to adequately safeguard customers' sensitive personal information. According to recent testimony by FTC Chairwoman Edith Ramirez, using the deceptive prong of its statute, the FTC has settled more than 30 matters challenging companies' express and implied claims about the security they provide for

---

[35] *Protecting Personal Consumer Information from Cyber Attacks and Data Breaches*: *Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 113th Cong. 25 (Mar. 26, 2014), available at http://www.commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=082407f8-9740-4e43-b2d2-1520c5495014&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a.

[36] 15 U.S.C. §45.

[37] U.S. Federal Trade Commission, *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, available at http://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

[38] Fed. Trade Comm'n, Bureau of Consumer Protection, *Privacy & Data Security Update* (June 2014), http://www.ftc.gov/reports/privacy-data-security-update-2014. ("An overview of the FTC's enforcement, policy initiatives, and consumer outreach and business guidance in the areas of privacy and data security, from January 2013-March 2014.").

[39] 16 C.F.R. Part 314.

[40] CRS Report RS20185, *Privacy Protection for Customer Financial Information*, by (name redacted).

[41] 15 U.S.C. §1681.

[42] 15 U.S.C. §6502 *et seq.*

[43] Fed. Trade Comm'n, Bureau of Consumer Protection, *Privacy & Data Security Update* (June 2014), http://www.ftc.gov/reports/privacy-data-security-update-2014. ("An overview of the FTC's enforcement, policy initiatives, and consumer outreach and business guidance in the areas of privacy and data security, from January 2013-March 2014.").

consumers' personal data, and the FTC has also settled more than 20 cases alleging that a company's failure to reasonably safeguard consumer data was an unfair practice.[44] Because most of the FTC's privacy and data security cases, and almost all of its COPPA and GLBA cases, were resolved with settlements or abandoned, there are few judicial decisions addressing the FTC's authority to regulate the data security practices of companies which have suffered a data breach.[45]

In 2006, The FTC brought its first data security enforcement action[46] against the data broker ChoicePoint after ChoicePoint disclosed a data breach involving the personal information of 163,000 persons. ChoicePoint ultimately agreed to pay $10 million in civil penalties and $5 million in consumer redress to settle the FTC's charges.[47] The FTC settlement required ChoicePoint to implement new procedures to ensure that it provides consumer reports only to legitimate businesses for lawful purposes, to maintain a comprehensive information security program, and to obtain audits by an independent third-party security professional every other year for twenty years.[48] These measures are typical of the measures required of companies in the FTC's consent agreements to remedy failures to provide reasonable security protections.[49]

In 2014, the FTC pursued its 50th data security enforcement action. The complaint against GMR Transcription Services—an audio file transcription service that relies on service providers and independent typists to transcribe files for their clients, which include healthcare providers.[50] The FTC alleged that as a result of GMR's failure to implement reasonable security measures and oversee its service providers, at least 15,000 files containing sensitive personal information—including consumers' names, birth dates, and medical histories—were available to anyone on the Internet.[51] Under the terms of the FTC'S consent order with GMR, the company and its owners are prohibited from misrepresenting the extent to which they maintain the privacy and security of consumers' personal information; must establish an information security program that will protect

[44] *Protecting Personal Consumer Information from Cyber Attacks and Data Breaches* Hearing: Before the S. Comm. on Commerce, Science, and Transportation (Mar. 26, 2014). Available at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=1e1ef0a2-692d-415b-a6b2-fd93316305fb.

[45] Prior to the recent judicial decision in the pending *Wyndham* case (discussed below), only one case had previously resulted in a judicial decision when the Tenth Circuit upheld the FTC's authority under Section 5 to bring an action against a company that wrongfully collected and disseminated confidential information. *Fed. Trade Comm'n v. Accusearch* Inc., No. 08-8003 (10th Cir. June 29, 2009).

[46] *United States v. ChoicePoint, Inc*., No. 106-CV-0198 (N.D. Ga. Jan. 26, 2005), *available at* http://www.ftc.gov/os/caselist/choicepoint/0523069stip.pdf.

[47] Fed. Trade Comm'n, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress (January 26, 2006), available at http://www.ftc.gov/news-events/press-releases/2006/01/choicepoint-settles-data-security-breach-charges-pay-10-million.

[48] *United States v. ChoicePoint, Inc*., No. 106-CV-0198 (N.D. Ga. Feb. 15, 2006), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2006/01/stipfinaljudgement.pdf.

[49] See, e.g., Dave & Buster's, Inc., No. C-4291 (F.T.C. May 20, 2010) (consent order), available at http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2010/06/dave-busters-incin-matter; DSW, Inc., No. C-4157 (F.T.C. Mar. 7, 2006) (consent order), available at http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2006/03/dsw-incin-matter; BJ's Wholesale Club, Inc., No. C-4148 (F.T.C. Sept. 20, 2005) (consent order), available at http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2005/09/bjs-wholesale-club-inc-matter; The TJX Cos., Inc., No. C-4227 (F.T.C. July 29, 2008) (consent order), available athttp://www.ftc.gov/enforcement/cases-and-proceedings/cases/2008/08/tjx-companies-inc-matter.

[50] Fed. Trade Comm'n, Provider of Medical Transcript Services Settles FTC Charges That It Failed to Adequately Protect Consumers' Personal Information (January 31, 2014), available at http://www.ftc.gov/news-events/press-releases/2014/01/provider-medical-transcript-services-settles-ftc-charges-it.

[51] GMR Transcription Servs., Inc., Matter No. C-4482 (F.T.C. Aug. 14, 2014) (complaint), available at http://www.ftc.gov/system/files/documents/cases/140821gmrcmpt.pdf.

consumers' sensitive personal information; and must have the program evaluated every two years by a certified third party.[52] The settlement will be in force for 20 years.

Many other companies have been subjected to FTC data security enforcement actions under its Section 5 authority. Recently, the FTC announced that it is also investigating the Target data breach.[53]

FTC v. Wyndham Worldwide Corp.

FTC v. Wyndham Worldwide Corp. is widely viewed as an important case to test the authority of the FTC to respond to data breaches, and it could have far-reaching implications for the liability of companies whose computer systems suffer a data breach.[54] After a data breach occurred involving the personal information of Wyndham Hotels and Resorts' customers in 2012, the FTC filed suit against the hotel chain and three of its subsidiaries, alleging that Wyndham's privacy policy misrepresented the security of customer information and that its failure to safeguard personal information caused substantial consumer injury. Specifically, the FTC alleged that wrongly configured software, weak passwords, and insecure computer servers led to three data breaches by at Wyndham hotels from 2008 to 2010, compromising more than 619,000 payment card accounts and transfer of customers' payment card account numbers to Russia. The FTC alleged that the computer intrusions led to more than $10.6 million in fraud losses. The agency ultimately alleged that Wyndham's security practices were "unfair and deceptive" in violation of Section 5 of the FTC Act.

Rather than settle the case as other companies facing FTC complaints have done, Wyndham contested the allegations and argued, among other things, that the FTC had exceeded its statutory authority to assert an unfairness claim in the data security context. Wyndham relied on the Supreme Court's ruling in *Food and Drug Administration v. Brown & Williamson Tobacco Corp.*,[55] which held that the Food and Drug Administration (FDA) could not utilize its *general* authorities with respect to drugs to mandate disclaimers on tobacco packaging because of the lack of *explicit* legal authority over tobacco products. The *Brown & Williamson* Court reached such a conclusion because, among other reasons, (1) the agency had disclaimed authority over tobacco products in the past;[56] (2) the FDA's authorizing statute did not clearly indicate the agency had such authority;[57] (3) Congress had already passed tobacco-specific legislation in the past without giving the FDA such authority;[58] and (4) it appeared unlikely that Congress would delegate a policy decision of such economic and political magnitude to the FDA through its general authority to regulate drugs.[59] In *Wyndham,* the hotel chain, relying on *Brown & Williamson,* argued that just as Congress did not grant the FDA through its general authority to regulate drugs

[52] GMR Transcription Servs., Inc., Matter No. 112-3120 (F.T.C. Dec. 16, 2013) (proposed consent order), available at http://www.ftc.gov/news-events/press-releases/2014/01/provider-medical-transcript-services-settles-ftc-charges-it.

[53] CRS Report R43496, *The Target Data Breach: Frequently Asked Questions*, by (name redacted) and (name redacted).

[54] Grande, Allison, *Wyndham Can't Shake FTC Data-Security Suit*, Law360 (Apr. 7, 2014), available at http://www.law360.com/articles/525903.

[55] 529 U.S. 120 (2000).

[56] *Id*. at 144.

[57] *Id.* at 133-43.

[58] *Id.* at 155-56.

[59] *Id.* at 160-61.

the specific authority to regulate tobacco products, Congress likewise did not give the FTC the necessary authority to regulate data security through the FTC's general authority to regulate unfair or deceptive trade practices. In making this argument, Wyndham noted the FTC's lack of clear statutory authority over data security; that the FTC had previously disclaimed its authority over data security; and, that Congress has enacted narrowly tailored data security legislation in FCRA, GLBA, and COPPA without providing the FTC with any broader authority. Moreover, Wyndham argued that it was unlikely that Congress would delegate a policy decision of such economic and political magnitude as setting data security standards through so general a delegation as the FTC's unfairness authority. In addition, Wyndham cited the Obama Administration's recent release of a cybersecurity framework[60] by the National Institute of Standards and Technology (NIST) as evidence that Congress did not provide the FTC with authority to regulate data security.

The FTC, in response, made several arguments. First, the agency argued that *Brown & Williamson* was distinguishable because here the agency's assertion of authority would not result in any statutory inconsistencies. The agency explained that the FTC Act provided the agency with a baseline authority to act in unfairness cases where it can prove substantial harm to consumers and asserted that regulating data security was consistent with that broad authority. Second, the FTC contended that specific data security laws like FCRA or HIPPA do not displace the FTC's authority, but instead supplement the FTC's Section 5 authority; grant the FTC additional powers; and affirmatively compel the FTC to use its consumer protection authority in specified ways, unlike the FDA's earlier disclaimer of authority to regulate tobacco. The FTC also argued that it had never disclaimed its "unfairness" authority over data security. Finally, the FTC claimed that any question about the FTC's authority in the data security context was put to rest by the recent decision in the FTC's administrative action against *LabMD* (discussed below).

On April 7, 2014, a federal district court judge in New Jersey, in *FTC v. Wyndham Worldwide Corp.,*[61] denied Wyndham's motion to dismiss the case, rejecting Wyndham's position that the FTC lacked statutory authority to regulate data security. Although the judicial opinion did not address the merits of whether Wyndham's security policies were inadequate, the judge did undertake, in a 42-page opinion, an in-depth analysis of the authority of the FTC to regulate data security. The district court in *Wyndham* began by noting that it was not ruling on a finding of liability, but only on the validity of FTC's legal theory of liability. The district court also cautioned that it was not handing the FTC a "blank check" to go after every company that suffers a data breach. As to Wyndham's claim that the FTC's unfairness authority does not include data security, the district court distinguished *Wyndham* from the *Brown & Williamson* reasoning. The court noted that in *Brown & Williamson* Congress had clearly intended to exclude tobacco products from FDA enforcement, whereas the case before it the court found no such congressional intent to create a data security carve out from the FTC's unfairness authority under Section 5 of the FTC Act. In fact, the court recognized that data security was a rapidly evolving area, and that nothing in Congress's several specific data security enactments (e.g., the FCRA, GLBA, and the COPPA) contradict or are otherwise incompatible with holding that the FTC possesses authority to enforce data security as an unfair trade practice under the FTC Act.

[60] Dep't of Commerce, "*Framework for Improving Critical Infrastructure Cybersecurity,"* (Feb. 12, 2014), http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf. For more background, see CRS Legal Sidebar, National Institute of Standards and Technology Issues Long-awaited Cybersecurity Framework (Mar. 5, 2104), http://www.crs.gov/LegalSidebar/details.aspx?ID=829&Source=search.

[61] *FTC v. Wyndham Worldwide Corp.,* Civil Action No. 13-1887 (ES) (D.N.J. Apr. 7, 2014).

Wyndham moved for and was granted permission to appeal the district court's ruling.[62] It is uncertain when a decision from the Third Circuit can be expected.

In the Matter of LabMD

In the Matter of LabMD[63] involves another challenge to the authority of the FTC to regulate data security breaches as unfair trade practices under the FTC Act. As was the case in *Wyndham,* the FTC's authority to bring enforcement actions for data security breaches was challenged, and in this instance, the commission found that the FTC had authority to bring such enforcement actions. However, unlike in *Wyndham,* the administrative hearing resulted in something sought by a defendant company: an order issued by the ALJ compelling the FTC to explicitly disclose what kinds of data security measures it expected the company to take and rejecting the agency's argument that its existing general guidance was sufficient. [64]

In the Matter of LabMD began in 2013 when the FTC filed a complaint, through its administrative process, against a Georgia medical cancer diagnostics company, LabMD, Inc. Under the FTC Act, the FTC is authorized to initiate enforcement actions either through administrative or judicial processes.[65] The administrative complaint against LabMD alleged that the company failed to reasonably protect the security of 10,000 consumers' personal data, including medical information; that these practices harmed consumers; and that consequently LabMD engaged in unfair practices in violation of the FTC Act. LabMD argued in a motion to dismiss that the FTC has no authority to address private companies' data security practices as unfair practices because the lab is a Health Insurance Portability and Accountability Act (HIPAA) covered entity.

In January 2014, four commissioners, on behalf of the FTC, unanimously denied LabMD's motion to dismiss and concluded that the FTC Act's prohibition of unfair practices applies to a company's failure to implement reasonable and appropriate data security measures.[66] According to the order denying LabMD's motion, the commission's authority to regulate data security practices to determine which practices are unfair was consistent with the FTC Act and its legislative history, other statutes, and extensive case law. The commission further asserted that legislative history of the FTC Act demonstrated that Congress decided to delegate broad authority to the commission to determine what practices were unfair. The commission likewise rejected LabMD's contention that Congress, by enacting more specific data security statutes, implicitly repealed the FTC's preexisting authority to enforce Section 5 of the FTC Act in the field of data security. The commission, noting that "[t] he cardinal rule is that repeals by implication are not favored," found nothing in HIPAA or any of the other cited statutes that reflected a "clear and

[62] *FTC v. Wyndham Worldwide Corp*., Civil Action No. 13-1887 (ES) (D.N.J. June 23, 2014), 2014 U.S. Dist. LEXIS 84914; 2014-1 Trade Cas. (CCH) P78,817.

[63] *LabMD, Inc.*, Docket No. 9357, 2014 FTC LEXIS 2; 2014-1 Trade Cas. (CCH) P78,784, (Jan. 16, 2014).

[64] *LabMD*, Inc., Docket No. 9357 (May 1, 2014), available at http://www.ftc.gov/system/files/documents/cases/140501labmdordercompel.pdf.

[65] U.S. Federal Trade Commission, *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, available at http://www.ftc.gov/about-ftc/what-we-do/enforcement-authority, http://www.ftc.gov/about-ftc/what-we-do/enforcement-authority.

[66] *LabMD, Inc.*, Docket No. 9357, 2014 FTC LEXIS 2; 2014-1 Trade Cas. (CCH) P78,784, (Jan. 16, 2014).

manifest" intent of Congress to restrict the commission's authority over allegedly "unfair" data security practices.

The commission also rejected LabMD's argument that the FTC's decision to proceed through adjudication without first conducting a rulemaking violates LabMD's constitutional due process rights.[67] According to the ruling, administrative agencies must enforce the statutes that Congress has directed them to implement regardless of whether they have issued regulations addressing the specific conduct. The FTC ultimately found the three-part[68] statutory standard governing whether an act or practice is "unfair" sufficient to provide fair notice of what conduct is prohibited. In reaching that conclusion, the commission noted that given the difficulty of drafting generally applicable regulations in this rapidly changing area, questions relating to data security practices in an online environment are particularly well-suited to case-by-case development in enforcement proceedings.

After the FTC Commissioners affirmed the agency's authority to sue,[69] the case's focus shifted to whether the FTC must disclose the data security standards it uses to determine whether a company's efforts to protect consumers' information could be considered reasonable. In the same proceeding, LabMD accused the FTC of holding the company to data security standards that do not exist officially at the federal level.[70] In response, the FTC argued that it should not be required to disclose the standards it uses to determine whether a company's data security practices are unfair under the FTC Act because of legal privileges. In May 2014, the FTC's Chief Administrative Law Judge ruled that the FTC can be compelled to disclose the data security standards it uses to determine whether a company has reasonable security measures. The administrative law judge ultimately held that the company has the right to know what data security standards the commission uses when pursuing enforcement actions. The judge ordered[71] the FTC to provide deposition testimony as to what data security standards, if any, have been published by the FTC which it intends to rely on at trial. The FTC's testimony will present companies with the first opportunity to obtain more specificity from the agency about the data security standards driving the FTC's data breach enforcement actions.

Proposed Legislation

As part of efforts to enact cyber[72] and data security[73] legislation, several bills before Congress include provisions that would provide the FTC with enhanced enforcement authority by, for

[67] *LabMD, Inc.*, Docket No. 9357, 2014 FTC LEXIS 2; 2014-1 Trade Cas. (CCH) P78,784, (Jan. 16, 2014).

[68] Under Section 5 of the FTC Act, an act or practice is unfair if the act or practice (1) "causes or is likely to cause substantial injury to consumers," (2) "which is not reasonably avoidable by consumers themselves," and (3) "not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. §45(n).

[69] The company had challenged the proceeding in the Eleventh Circuit and the Northern District of Georgia, claiming the commission lacks authority to regulate private companies' data security. Both courts deferred to the ongoing administrative enforcement actions.

[70] *LabMD*, Inc., Docket No. 9357 (May 1, 2014), available at http://www.ftc.gov/system/files/documents/cases/140501labmdordercompel.pdf.

[71] *LabMD*, Inc., Docket No. 9357 (May 1, 2014), available at http://www.ftc.gov/system/files/documents/cases/140501labmdordercompel.pdf.

[72] CRS Report R43317, *Cybersecurity: Legislation, Hearings, and Executive Branch Documents*, by (name redacted).

[73] CRS Report R43496, *The Target Data Breach: Frequently Asked Questions*, by (name redacted) and (name redacted).

example, explicitly authorizing the FTC to promulgate rules to implement data security standards and to assess civil penalties. In recent FTC testimony[74] before Congress, the agency has called for federal legislation that would (1) strengthen its existing authority governing data security standards on companies and (2) require companies to provide notification to consumers where there is a data security breach. In both of those areas the FTC seeks the ability to impose civil penalties and the authority to issue administrative rules.

Several bills have been introduced in the Senate in the 113th Congress that could, in varying ways, impact the FTC's powers. S. 1193 (Senator Toomey), S. 1897 (Senator Leahy), S. 1927 (Senator Carper and Senator Blunt), S. 1976 (Senator Rockefeller), and S. 1995 (Senator Blumenthal) would expressly give the FTC the power to levy civil penalties with respect to companies that fail to comply with certain data security standards. S. 1897 would permit the FTC to impose civil penalties for violations for failing to comply with federal cybersecurity standards. S. 1976 would provide the FTC with explicit authority to promulgate "information security" regulations that could extend to certain non-profits. The bill would further allow the FTC to enforce violations of these regulations with various civil penalties. Likewise, S. 1995 would give enforcement authority to the FTC.

Author Contact Information

(name redacted)
Legislative Attorney
[redacted]@crs.loc.gov, 7-....

[74] *Protecting Personal Consumer Information from Cyber Attacks and Data Breaches* Hearing: Before the S. Comm. on Commerce, Science, and Transportation (Mar. 26, 2014). Available at http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=1e1ef0a2-692d-415b-a6b2-fd93316305fb.