April 20, 2015

Weil

Alert
Cybersecurity, Data Privacy & Information Management

Cybersecurity Enforcement: The FTC Is Out There

By Robert Carangelo, Eric Hochstadt, and Gaspard Curioni

The continued occurrence of serious data breaches, including the hack of Sony Pictures that resulted in the canceled theatrical release of *The Interview*, a satirical film about North Korean leader Kim Jong-un, and the Target data theft impacting up to 110 million consumers and several financial institutions, has put a spotlight on issues of cybersecurity and the protection of sensitive personal information. With public pressure mounting due to this growing threat, Congress is considering legislative action to bolster American businesses' resilience to cybersecurity attacks and data theft.[1] But while the political process on Capitol Hill unfolds, other branches of the federal government have not remained idle. In the executive branch, the Federal Trade Commission (FTC) has stepped up its consumer protection enforcement activity in this area and has pursued actions against companies that the agency deems do not sufficiently protect personal data.

Overview of the FTC's Cybersecurity Enforcement Authority and Actions

While the FTC has brought more than 50 enforcement proceedings in the past 15 years relating to data security, the pace of FTC activity has picked up in recent years.[2] The bulk of the agency's enforcement has been carried out through administrative actions, which in almost all instances[3] have been resolved through consent orders that impose data security measures and long-term supervision by the FTC. The remaining dozen or so cases brought by the FTC have been filed in federal courts pursuant to the agency's injunctive authority under section 13(b) of the Federal Trade Commission Act (FTC Act). As discussed further below, the FTC has brought such an enforcement action against the Wyndham hotel group, a case pending at the Third Circuit which is expected to address the reach of the FTC's authority in this area. As with administrative actions, the overwhelming majority of these cases settle shortly after filing. For companies under investigation, early settlement may be driven by, among other considerations, a desire to avoid protracted litigation with a federal agency. Administrative and judicial proceedings involve intrusive and costly discovery[4] and can take years to resolve.[5]

The FTC's enforcement authority derives principally from the FTC Act.[6] Under section 5(a) of the FTC Act, the FTC may take action against "unfair or

deceptive acts or practices in or affecting commerce." Historically, the agency has leveraged the FTC Act's "deception" prong to challenge allegedly false data security representations made by companies. Up until 2014, all but one cybersecurity civil action brought by the FTC and more than half of FTC data security administrative actions invoked the deception prong.[7] More recently, the FTC has challenged cybersecurity practices under the "unfairness" prong of section 5 of the FTC Act. In these enforcement actions, the FTC has developed minimum cybersecurity standards for companies that collect personal information, even in the absence of any allegedly false representations concerning data security.

Many data security vulnerabilities have drawn the agency's attention as being "unfair" to consumers, including companies' alleged failure to:

1. set up robust log-in protocols;[8]
2. protect against "commonly known or reasonably foreseeable attacks from third parties attempting to obtain access to customer information;"[9]
3. encrypt data;[10] and
4. provide cybersecurity training.[11]

Through its consent decrees, the FTC has detailed the various steps that companies must implement to remedy these deficiencies. The typical consent orders, which usually last for 20 years, prohibit prospective misrepresentations concerning data security and prescribe affirmative security measures. A central requirement is the establishment of a comprehensive information security program with administrative, technical, and physical safeguards suitable for the company and the type of protected data. Further, the consent orders usually require independent risk assessments from information technology and security professionals, as well as periodic reporting of the findings to the FTC. Companies must also document their compliance efforts and report material changes affecting their obligations to the agency.

FTC v. Wyndham Worldwide Corp.

There has been little judicial scrutiny of the FTC's exercise of its section 5 power in the cybersecurity space. A notable exception is *FTC v. Wyndham Worldwide Corp.*,[12] a case which may at last provide much-needed clarification about the scope of the FTC's authority to impose cybersecurity standards in the absence of substantive statutes or regulations on the subject.

In June 2012, the FTC sued Wyndham, alleging that it failed to maintain "reasonable and appropriate" data security measures. The failure purportedly allowed hackers to gain access to its computer networks, which resulted in the compromise of more than 500,000 payment card accounts and fraudulent charges on hotel guests' accounts. Because Wyndham allegedly misrepresented that it had implemented reasonable data protection measures on its website, the agency claimed that Wyndham had engaged in deceptive practices under section 5 of the FTC Act. However, the FTC did not stop there. It also claimed that Wyndham violated the unfairness prong of section 5 by failing to implement "reasonable and appropriate" data protection measures in the first place.

In seeking dismissal of the unfairness claim, Wyndham contended that section 5's unfairness prong did not confer the FTC with rulemaking authority over data security. A New Jersey federal judge rejected that argument in April 2014, given section 5's broad language and the absence of any statutory command carving out cybersecurity from the FTC's purview. But because of the novelty and importance of the issue, the judge certified the question for immediate appeal to the Third Circuit. On appeal, Wyndham argued that a business's failure to take "reasonable and appropriate" cybersecurity measures was not an unfair practice under section 5, as it was not an attempt to take advantage of customers; rather, a cyber-attack harmed the company. Wyndham also faulted the FTC for failing to adequately specify what were "reasonable and appropriate" cybersecurity practices. During oral argument on March 3, 2015, the Third Circuit panel questioned whether the unfairness prong covered nonfraudulent negligent cybersecurity conduct and whether the FTC could directly bring an action in court without first issuing cybersecurity rules through rulemaking or adjudication. The court heard oral arguments on the latter issue on March 27, 2015.

The upcoming ruling by the Third Circuit will likely provide greater clarification about the scope of the FTC's unfairness authority over cybersecurity practices.

Parallel and Follow-On Litigation

To date, the FTC's enforcement actions in the cybersecurity arena have not led to a wave of private follow-on litigation. One possible explanation is that the FTC Act, unlike the federal antitrust statutes enforced by the FTC, does not confer a private right of action. Enforcement targets must nevertheless be vigilant. Even if not subject to private litigation under the FTC Act, cybersecurity practices that the FTC deems unfair or deceptive can also lead to private follow-on class action litigation by consumers and other affected parties under state laws, such as consumer protection statutes or specific state data security statutes.[13]

The CBR Systems controversy is one such example of parallel FTC enforcement and private consumer litigation. CBR is a California-based company that stores stem cells from umbilical cord blood and tissue. In December 2010, a thief broke into a CBR employee's car and stole a backpack containing a company laptop computer and other electronic storage devices that allegedly held unencrypted personal information on about 300,000 CBR clients, including their names, addresses, social security numbers, medical history, and payment details. The FTC opened an investigation and ultimately filed an administrative complaint in January 2013, asserting that CBR had engaged in deceptive practices by failing to protect its customers' personal data. Shortly after, CBR entered into a 20-year consent order in which it agreed to establish and maintain a comprehensive information security program, be subject to monitoring from an independent auditor, and report periodically to the FTC about its cybersecurity efforts.[14] But the FTC consent order did not end CBR's travails. In January 2012, clients of CBR filed a putative class action under California privacy and unfair competition law. The case settled in February 2013, with CBR agreeing to reimburse affected clients for identity theft-related losses, pay for class members' two-year subscription to a credit monitoring program, and pay $600,000 in attorneys' fees. The full value of the class settlement was estimated at $112 million.[15]

Companies must also watch out for parallel litigation by state attorneys general. Snapchat's case is illustrative. Snapchat's mobile messaging application allows users to send photo and video messages (termed "snaps") that the company claims disappear very shortly after being sent. Despite the claimed "ephemeral" nature of the snaps, recipients were able to use third-party tools to save the snaps indefinitely. In May 2014, the FTC filed a complaint against Snapchat, alleging that the company made false representations about the disappearance of the snaps, the collection of users' personal data, and the robustness of its data security. Based on these allegations, the FTC asserted that Snapchat had engaged in deceptive practices under section 5 of the FTC Act. In May 2014, Snapchat agreed to settle with the FTC. The consent order prohibited misrepresentations about the company's data privacy and security, required Snapchat to establish a comprehensive privacy program, and imposed independent monitoring and reporting obligations for 20 years.[16] While the FTC enforcement action was pending, the Maryland attorney general advanced similar allegations against Snapchat and claimed violations of Maryland consumer protection law and COPPA. Snapchat agreed to pay $100,000 and take corrective measures in a June 2014 settlement with Maryland.

Finally, FTC investigations and enforcement proceedings may expose companies to follow-on litigation beyond the consumer protection context. For example, as a result of the FTC's enforcement action against Wyndham, the company was hit with a shareholder derivative suit which alleged that Wyndham's directors and officers failed to implement adequate data-security measures and timely disclose the data breaches.[17] Although the lawsuit was ultimately dismissed at the pleading stage, the case shows the potential spillover effect of FTC enforcement proceedings. A comprehensive defense strategy should include close coordination between data protection and securities counsel.

Conclusion

Cybersecurity law enforcement is growing. While legislative momentum is building toward formulating federal data security standards, the FTC has continued to use its enforcement authority over unfair and deceptive trade practices to bring cases against companies with allegedly substandard data security practices. Critics point out that the agency does not have any regulatory authority over data security and that the general principles contained in its various consent orders do not provide sufficient guidance to the industry. The Third Circuit is expected to develop the law in this area in the coming months, but it undoubtedly will not be the final word. In the meantime, companies are well advised to bolster their cybersecurity practices and get ahead of any issues that could subject them to the full panoply of FTC enforcement action followed by state regulatory or private class action litigation.

1. *See* Discussion Draft (Mar. 20, 2015), Data Security and Breach Notification Act of 2015, H.R. ___, 114th Cong. (2015); Personal Data Privacy and Security Act of 2014, H.R. 3990, 113th Cong. (2014).
2. *Legal Resources*, Filtered by Type (Case) and Topic (Data Security), FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field_consumer_protection_topics_tid=249 (last visited Apr. 1, 2015). Based on a review of publicly available data on the FTC website, twice as many administrative proceedings and court cases were initiated in the last five years as in the previous ten years. *See id.* A record number – seven administrative proceedings and two federal court cases – were brought in 2014 alone. *See id.*
3. Only one company, LabMD, Inc., has refused to enter into a consent decree with the FTC. *See id*. The FTC filed an administrative complaint against the company for its alleged failure to establish reasonable data security measures to protect customer information. After the FTC denied LabMD's motion to dismiss, the company sought review of the decision in federal court. The Court of Appeals for the Eleventh Circuit ultimately rejected LabMD's challenge as unripe because the FTC's decision was a non-final agency action. The case has been remanded to the FTC and is currently pending before an administrative law judge. *See Case Timeline, In re LabMD*, FTC File No. 102 3099, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/cases-proceedings/102-3099/labmd-inc-matter (last updated Feb. 24, 2015).
4. *See* 16 C.F.R. §§ 3.31-40 (setting out the methods, scope, and types of discovery in FTC administrative proceedings).
5. *See Case Timeline, In re LabMD, supra* note 3.
6. In addition, the FTC is entrusted with enforcing the privacy and data security provisions of specific statutes. Before the creation of the Consumer Financial Protection Bureau in 2011, the FTC was responsible for enforcing the Fair Credit Reporting Act (FCRA) – which ensures that credit reporting agencies protect consumers' private information – and the Gramm-Leach-Bliley Act (GLBA) – which obliges financial institutions to ensure the security of customer records. Also, the FTC administers the Children's Online Privacy Protection Act of 1998 (COPPA), which requires Internet companies to obtain parental consent for the collection, use, and disclosure of children's personal information. Finally, the Safe Harbor Framework program, which allows companies to transfer personal data between the United States and the European Union, provides for FTC enforcement against companies that fail to comply with the program's requirements.
7. *See Legal Resources, supra* note 2.
8. *See, e.g.*, Complaint at 2, *In re TJX Cos.*, FTC File No. 072-3055, Docket No. C-4227 (F.T.C. July 29, 2008), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2008/08/080801tjxcomplaint.pdf.
9. Complaint at 6, *United States v. RockYou, Inc.*, No. 3:12-cv-01487 (N.D. Cal. Mar. 26, 2012).
10. *See, e.g.*, Complaint at 9, *FTC v. LifeLock, Inc.*, No. 2:10-cv-00530 (D. Ariz. Mar. 9, 2010).
11. *See, e.g.*, Complaint at 2, *In re EPN, Inc.*, FTC File No. 112 3143, Docket No. C-4370 (F.T.C. Oct. 3, 2012), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026epncmpt.pdf.
12. No. 2:13-cv-01887 (D.N.J. transferred Mar. 26, 2013). After denying Wyndham's motion to dismiss, the district court certified its order for interlocutory appeal on June 23, 2014. The case is currently pending before the Third Circuit Court of Appeals. *See FTC v. Wyndham Worldwide Corp.*, No. 14-3514 (3d Cir. argued Mar. 3, 2015).
13. *See, e.g.*, Notice of Removal, *Johansson-Dohrmann v. CBR Systems, Inc.*, No. 3:12-cv-01115 (S.D. Cal. May 7, 2012), ECF No. 1-3 (attaching the class action complaint originally filed in state court, which alleged violations of the California Confidentiality of Medical Information Act and Unfair Competition Law, among other causes of action).

14. Decision & Order, *In re CBR Systems, Inc.*, FTC File No. 112 3120, Docket No. C-4400 (F.T.C. Apr. 29, 2013), *available at* https://www.ftc.gov/sites/default/files/documents/cases/2013/05/130503cbrdo.pdf.
15. *See* Order Granting Final Approval of Class Action Settlement, Attorneys' Fees, Costs, and Incentive Award, Judgment and Dismissal, *Johansson-Dohrmann*, No. 3:12-cv-01115 (July 24, 2013), ECF No. 35.
16. Decision & Order, *In re Snapchat, Inc.*, FTC File No. 132 3078, Docket No. C-4501 (F.T.C. Dec. 23, 2014), *available at* https://www.ftc.gov/system/files/documents/cases/141231snapchatdo.pdf.
17. *See Palkon v. Holmes*, No. 2:14-cv-01234, 2014 WL 5341880, at *6 (D.N.J. Oct. 20, 2014).

Cybersecurity, Data Privacy & Information Management is published by Weil, Gotshal & Manges LLP, 767 Fifth Avenue, New York, NY 10153, +1 212 310 8000, www.weil.com.

If you have questions concerning the contents of this issue, or would like more information about Weil's Cybersecurity, Data Privacy & Information Management practice, please speak to your regular contact at Weil, or to the editors or authors listed below:

Editors:

Michael Epstein (NY)	Bio Page	michael.epstein@weil.com	+1 212 310 8432
Randi Singer (NY)	Bio Page	randi.singer@weil.com	+1 212 310 8152
Paul Ferrillo (NY)	Bio Page	paul.ferrillo@weil.com	+1 212 310 8372

Contributing Authors:

Robert Carangelo (NY)	Bio Page	robert.carangelo@weil.com	+1 212 310 8499
Eric Hochstadt (NY)	Bio Page	eric.hochstadt@weil.com	+1 212 310 8538
Gaspard Curioni (NY)	Bio Page	gaspard.curioni@weil.com	+1 212 310 8068