BUSINESS LAW TODAY

Cyber Center:

Cybersecurity as an Unfair Practice: FTC Enforcement under Section 5 of the FTC Act

By William R. Denny

Cyber attacks seem only to be increasing in frequency and severity. Major data breaches suffered by companies such as Target, Sony, Anthem Health Care, and others, have exposed hundreds of millions of individuals to the risk of credit loss and identity theft. Virtually all industries have been targeted. Moving past credit cards, cybercriminals are increasingly going after proprietary business data and deploying ransomware and cyber blackmail. They are holding data hostage and attempting to extort millions of dollars from companies who wish to avoid the risk of data loss and public embarrassment. Often, attackers find their way to company data through vendors, who provide technical or financial services or through targeted e-mail attacks directly on company employees, using social exploits to induce unsuspecting individuals to open e-mail attachments and download malware. Companies who are victims of these attacks have suffered huge financial losses. According to the Ponemon Institute in 2015, the total average cost of a data breach is now $3.8 million, up from $3.5 million a year earlier, or $154 per individual record lost or compromised. These costs do not even include other, less direct costs, such as the loss of business or reputational damage.

In spite of growing concern about cybersecurity, Congress has not yet adopted broad federal legislation. Instead, companies today face a patchwork of laws and regulations pertaining to corporate cybersecurity practices, including 47 states and the District of Columbia, as well as multiple federal agencies. Many federal agencies involved in cybersecurity regulation are industry-specific, focusing, for example, on financial services, on healthcare, on insurance or on publicly-traded corporations. However, one agency, the Federal Trade Commission (FTC), has taken a broad mandate to extend its oversight over all companies operating in the United States. Since 2002, the FTC has assumed a leading role in policing corporate cybersecurity practices. In that time, it has brought more than 60 cases against companies for unfair or deceptive practices that endanger the personal data of consumers.

Given the increasingly important role of the FTC in policing cybersecurity, companies would be well-advised to examine whether their cybersecurity practices and policies may subject them to regulatory action by the FTC in the event of a data breach. Without prescriptive regulations to assure that their conduct falls within a safe harbor, companies face uncertainty in determining what or how much they should do to avoid an FTC enforcement action. Companies should look to guidance published by the FTC and other regulatory agencies to determine whether their current cybersecurity practices appear reasonable and to develop and update their policies for responding to and recovering from a data breach.

FTC Has New Mandate to Regulate Cybersecurity

Section 5 of the FTC Act, dating back to 1914, prohibits "unfair or deceptive business practices in or affecting commerce." Not surprisingly for a law passed in 1914, the act does not mention cybersecurity. However, the FTC has long maintained that Congress intended for the word "unfair" to be interpreted broadly and flexibly to allow the agency to protect consumers as technology changes. Most early consumer privacy cases brought by the FTC came under the "deception" prong of Section 5. They targeted companies that gave false data security or privacy representations to their customers through websites or other applications. In 2002, the FTC started asserting claims based on "unfair" cybersecurity practices. For the next 10 years, all actions brought by the FTC resulted in negotiated consent agreements, with no company testing the

FTC's statutory authority to regulate cybersecurity. While some companies questioned the FTC's authority, they all settled rather than engage in an embarrassing legal battle. That changed when the FTC sued Wyndham Worldwide Corp. in 2012.

The FTC alleged that hackers had obtained unauthorized access to Wyndham's computer networks on three separate occasions. The incidents exposed more than 600,000 consumer payment card numbers and led to more than $10.6 million in fraudulent charges. Rather than settle, Wyndham moved to dismiss the complaint on the bases that (1) the FTC had no authority, (2) the "unfairness" prong of Section 5 of the FTC Act did not encompass unreasonable data security measures, (3) the FTC had not given companies notice of how their level of data security could be deemed an unfair trade practice, and (4) the FTC did not sufficiently allege consumer injury. The district court denied Wyndham's motion, but certified its decision on the "unfairness" prong of Section 5 to allow interlocutory appeal to the Third Circuit.

In *FTC v. Wyndham Worldwide Corp.*, 799 F. 3d 236 (3d Cir. 2015), the Third Circuit affirmed that the FTC has authority to regulate cybersecurity. The Third Circuit held that Section 5 was not impermissibly vague. Congress had explicitly rejected the notion that specific "unfair" practices should be enumerated in the act. According to Section 5(n) of the FTC Act, to be deemed "unfair," (1) an act must be likely to cause "substantial injury" to consumers, (2) consumers cannot reasonably avoid the injury, and (3) the injury is not outweighed by benefits to consumers or competition. The language thus informs parties that the relevant inquiry is a cost-benefit analysis. Wyndham also argued to the Third Circuit that when a business itself is the victim of a cyber attack, it does not treat its customers in an "unfair" manner. The court rejected this argument, explaining that the FTC Act expressly contemplates the possibility that unfair conduct could take place before an actual injury occurs. Thus, the fact that Wyndham was a victim of criminal activity did not immunize it from liability where injury to its customers was foreseeable. Wyndham's conduct need not have been the proximate cause of the injury for the company to be liable for foreseeable harm, because, after the first attack, the second and third attacks were no longer unforeseeable.

Wyndham challenged the FTC's complaint also on the basis that it did not have fair notice as to what cybersecurity practices would fall short under the "unfairness" prong of Section 5. This argument was a stretch, as Wyndham's cybersecurity practices, if they could be called such, were nothing short of egregious. Wyndham had been hacked not one but three times. It had failed to use firewalls, did not restrict IP addresses, failed to use encryption for sensitive customer files like credit card information, and did not require users to change default passwords on network equipment. Predictably, the Third Circuit held that notice was constitutionally sufficient "as long as the company can reasonably foresee that a court could construe its conduct as falling within the meaning of the statute." The court pointed to several FTC publications and administrative enforcement actions that put Wyndham on notice that its practices were unlikely to survive the cost-benefit analysis under the "unfairness" prong of the FTC Act. Specifically, the court pointed to a 2007 FTC guidebook titled *Protecting Personal Information: A Guide for Business*, which described a checklist of practices that formed a sound data security plan and advised against many of the very practices of which Wyndham was guilty. Additionally, the court indicated that the FTC's published complaints and consent decrees in cases raising unfairness claims had close factual corollaries and so should also have put Wyndham on notice.

Following affirmance of the FTC's authority, Wyndham and the FTC reached a settlement in December 2015, under which Wyndham agreed to establish a comprehensive information security program designed to protect cardholder data. Wyndham must also conduct annual information security audits, the benchmark being the Payment Card Industry Data Security Standard, which generally applies to credit card processors. These and other obligations under the agreement will last 20 years. The settlement is noteworthy, in that the FTC laid out more specificity than is typical in its consent decrees, thus offering more guidance to companies as to what the FTC, at least today, considers "reasonable and necessary."

New Uncertainty over the Scope of FTC Authority

Like Wyndham, another company sued by the FTC for lax data security practices, LabMD, decided to fight back. LabMD was a clinical laboratory that conducted tests on samples and reported results back to physicians. It experienced two incidents that led to the FTC complaint. First, a third-party company contacted LabMD in 2008 and reported that it had found a LabMD report containing personal information on a peer-to-peer file sharing network. It turns out that this third-party company was angling to find private information on the internet and then offer security services to the affected business. Second, documents from LabMD containing personal information for at least 500 individuals were found in the hands of criminals charged with identity theft. Rather than sue in court, as the FTC did against Wyndham, the FTC issued an administrative complaint on August 28, 2013, after a three-year investigation of LabMD's cybersecurity practices. The FTC accused LabMD of an "unfair or deceptive" business practice, in that it allegedly had held private information without taking reasonable measures to secure it.

Various privacy groups took up the battle against the FTC on behalf of LabMD, and, following an evidentiary hearing before an administrative law judge, the judge on November 13, 2015, dismissed the administrative complaint. The core holding was that the FTC failed to prove substantial injury to consumers. The government had to prove "actual injury" to consumers, not merely a theoretical risk of future harm. Under Section 5(n), the FTC has no authority to declare an act or practice unlawful "unless the act or practice causes or is likely to cause substantial injury to consumers." The administrative law judge determined that the FTC could not meet this burden, as it could

not show that the alleged data breaches had caused tangible harm to anyone. The judge stated that, "[a]t best, [the FTC] has proven the 'possibility' of harm, but not any 'probability' or likelihood of harm. Fundamental fairness dictates that demonstrating actual or likely substantial consumer injury under Section 5(n) requires proof of more than the hypothetical or theoretical harm that has been submitted by the government in this case."

The FTC appealed the administrative law judge decision to its own commissioners, pressing its own view that "mere disclosure is harm" and "some risk is enough" to establish substantial injury. At oral argument on May 16, 2016, the FTC argued that "a significant risk of substantial harm [i.e., from failure to put reasonable security practices in place] is itself substantial injury" to consumers. This is an extreme position that would result in liability for unfair practices without any actual, concrete harm to a consumer having taken place. However, LabMD's position may be strengthened by the recent Supreme Court decision in *Spokeo, Inc. v. Robins*, No. 13-1339, 578 U.S. __ (May 16, 2016), holding that Article III standing to bring a claim requires injury-in-fact, which means that the injury must be "concrete and particularized."

It is likely the judge's opinion will be reversed by the commissioners, as the commissioners historically have sided with the FTC position, whether to uphold or overturn an administrative law judge, 100 percent of the time. However, when (not if) the decision is appealed to the U.S. District Court, the rationale of *Spokeo* may cause the court to dismiss the case due to the FTC's lack of Article III standing if it finds that there is no "concrete" injury to consumers, despite the FTC's alleged statutory authority under the FTC Act to bring the enforcement action.

Takeaways from the Wyndham and LabMD Decisions

In the absence of comprehensive data security legislation, the FTC will continue to use Section 5 to develop, on a case-by-case basis, the new common law of cybersecurity. It will assert such claims under both the "deceptive" and "unfairness" prongs of the act. The appeal in LabMD should determine whether the "deceptive" prong requires a showing that the conduct was "likely to cause substantial injury to consumers" and whether this is a sufficiently concrete injury to confer standing. Moreover, companies against whom the FTC brings enforcement actions will likely continue to settle and enter into consent decrees rather than litigate. Indeed, it is generally agreed that the FTC action against LabMD and its decision to challenge the FTC led to the company's demise, and few companies will wish to undertake such a risk. Finally, the LabMD ruling turned upon unique facts, especially the controversial tactics of the hacker, an alleged security business that was trolling for new clients in an unscrupulous way. Other companies cannot rely upon similar issues arising and interfering with the FTC investigation, and so will likely settle with the FTC.

Companies should be asking themselves whether their cyber security practices could reasonably be said to survive the cost-benefit analysis cited by the Third Circuit, by weighing the risks to their consumers presented by their cyber security practices against the benefits of such practices to consumers or competition. This analysis should also take the actual cost of the cyber security practices into account. Companies should consider whether their practices conform to current FTC guidance.

The standard of care the FTC has most recently articulated requires businesses to take "reasonable and necessary measures" to protect consumer data. The FTC has not provided bright line rules defining what constitutes "reasonable and necessary measures" for implementing a cybersecurity program, but it has provided guidance. The FTC website publishes guidelines, tips, and advice for businesses and past complaints and consent orders. See https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security.

On June 30, 2015, the FTC released a guide for businesses with practical tips and advice to help organizations better secure their data. The guide, *Start with Security: A Guide for Business*, draws on more than 50 data security enforcement actions by the FTC against various businesses. The FTC notes that, "the specifics of the cases apply just to those businesses, but each action offers compliance nuggets for other companies to consider. Building on its 2007 guidebook, the FTC encourages organizations to consider data security at the earliest possible stage and to make "reasonable choices based on the nature of their business and the sensitivity of the information involved." *Start with Security* distills important facts from prior cases into 10 common-sense lessons. Adhering to these standards should help businesses avoid an FTC enforcement action even if a data breach or loss occurs. These 10 lessons are:

1. Start with security. No one can steal what you don't possess. The FTC emphasizes that companies should not collect personal information that they do not need, and should hold on to information only so long as they have a legitimate business need.
2. Control access to data sensibly. Consider who really needs access to sensitive data and automate data access rules to detect suspicious user behavior.
3. Require secure passwords and authentication. The FTC recommends that companies insist on complex and unique passwords, store passwords securely, and protect against authentication bypass mechanisms.
4. Store sensitive personal information securely and protect it during transmission. Make sure encryption technologies are properly configured, deployed, and updated.
5. Segment your network and try to monitor who is trying to get in and out. Firewall tools are important, but so are intrusion detection and prevention monitoring tools.
6. Secure remote access to your network. Limit what can be accessed remotely, and secure the computers used to remotely access the network.
7. Apply sound security practices when developing new products. Train engi-

neers to use secure coding practices. Test and verify privacy features prior to deployment.

8. Make sure your service providers implement reasonable security measures. Third party providers and business partners should be required to sign agreements to provide appropriate security. Companies should have processes in place to actually verify that service providers are complying.
9. Put procedures in place to keep your security current and address vulnerabilities that may arise. Update third party software regularly. Put a process in place to allow for reporting of security vulnerabilities and taking corrective actions.
10. Secure paper, physical media, and devices. Keep important papers in a secure location and delete or destroy when no longer needed. Make sure digital devices are properly secured and are wiped when no longer needed.

FTC guidelines and cases may help form the standard for defining what constitutes "reasonable and necessary" security practices. The problem, however, is that the ten guidelines listed above are general and not prescriptive. There is no safe harbor where companies know that, by compliance with these standards, they are safe from FTC enforcement actions. The guidelines still leave significant uncertainties for companies that employ certain safeguards and not others.

Tips for Convincing Your Client to Take Action

Guarding against an FTC enforcement action means engaging in all "reasonable and necessary" security practices, including preparing to respond and remediate in the event of a data breach. As lawyers, we should remind our clients that cybersecurity is an enterprise-wide risk management issue, not just an IT issue. Cyber risks pose serious threats to business operations, including reputational injury, financial loss, damage to infrastructure, shareholder suits for breach of duty of care, and regulatory enforcement actions. Senior management must consider cybersecurity as part of its enterprise risk management duties. Company directors can be held individually liable for their failure to manage cyber risks adequately. In this environment, directors would be well-advised to begin thinking of cybersecurity as part of the fiduciary duty of care that they owe the company.

While the FTC does not provide checklist guidance, there are many other governmental agencies and private organizations that offer specific guidance. These include the National Institute of Standards and Technology, the National Labor Relations Board, the Financial Industry Regulatory Authority, the Department of Health and Human Services, the Department of Homeland Security, the Department of Defense, the U.S. Chamber of Commerce, the New York Department of Financial Services, and the Securities and Exchange Commission. Industry-specific and other federal laws with specific guidance include the Gramm Leach Bliley Act, the Fair Credit Reporting Act, Children's Online Privacy Protection Act, the Family Educational Rights and Privacy Act, the Electronic Communications Privacy Act, the Communications Act, and the Computer Fraud and Abuse Act. Companies should know the regulators that focus on their specific industry and use their guidance as a starting point. This plethora of standards and guidance demonstrates that standards are evolving, and that companies must monitor changes and strive for continuous improvement. The best way to demonstrate, in an FTC enforcement action, that a company has instituted "reasonable and necessary" security practices is to show a serious effort to follow and implement the evolving standards appropriate to that company's industry.

Company officials therefore should retain qualified, independent experts to evaluate the company's cyber-risk profile and provide specific recommendations. The FTC is making cybersecurity an enforcement priority, and it wants to see similar levels of commitment in companies. Companies should conduct in-depth evaluations of those recommendations, including discussion at the board level. The *Wyndham* case shows how simply raising the issue of cybersecurity at board meetings can help to reduce directors' liability and demonstrate due diligence. Directors should ask what their companies are doing in the area of cybersecurity. If organizations has designated a specific person as responsible for cybersecurity, that person should be invited to attend a board meeting, give a presentation with recommendations and answer questions. Also, companies should understand the legal implications of cybersecurity as they relate to the companies' specific circumstances. The Wyndham board's consultation with counsel was one factor that the Third Circuit found demonstrated good faith and diligence. With this information, companies should identify which risks to avoid, which to accept, and which to mitigate or transfer through insurance.

Good first steps toward better cybersecurity will begin to build protections from potential FTC enforcement actions in the event of breach. In conjunction with monitoring the evolving legal standards, companies should examine their data collection and determine whether they are storing sensitive information. They should identify their data retention, sharing and destruction policies and practices, evaluate network security, monitor network activity, restrict access to sensitive data, manage vendor security, develop an effective incident response plan and provide ongoing training to employees. Every organization should limit its risk by taking preventive measures and being prepared to respond to and mitigate any harm caused by an incident.

William R. Denny is partner at Potter Anderson Corron LLP in Wilmington, Delaware.