Bloomberg Law

White Collar Crime Report™

CYBERSECURITY

Two attorneys at Skadden, Arps, Slate, Meagher & Flom LLP survey the landscape of the FTC's cybersecurity enforcement procedures. The authors examine the FTC's basis for enforcement actions, resulting settlements, still-open legal questions, and provide several practice pointers.

Looking Backward to Look Forward: A Summary Of the FTC's Cybersecurity Enforcement Agenda

By Paul M. Eckles and Luke T. Taeschler

Paul M. Eckles is a partner at Skadden, Arps, Slate, Meagher & Flom LLP in New York. Eckles represents a wide variety of clients across numerous industries in antitrust, unfair business practices, consumer fraud, and other complex litigation matters at both the trial and appellate court levels. He can be reached at paul.eckles@skadden.com.

Luke T. Taeschler is an associate with Skadden in the firm's New York office. He can be reached at luke.taeschler@skadden.com.

Introduction

In August, Uber agreed with the Federal Trade Commission (''FTC'') to settle allegations that it had deceived consumers using the Uber application (Uber drivers, specifically) by inadequately protecting their personal information. Hailed as the first data-related settlement within the ''sharing'' economy, the settlement demonstrates the FTC's continued commitment to prosecuting cybersecurity cases, an enforcement agenda that has grown significantly over the last few years and shows no signs of slowing. Indeed, Bloomberg News recently announced that the Trump administration's FTC will not ''loosen the reins on data security and privacy enforcement,'' regardless of which individuals are appointed to lead the agency. Similarly, in an oral argument in June before the Eleventh Circuit, the FTC argued for an increasingly expansive reading of the Federal Trade Commission Act (''FTC Act'' or ''the Act''), which would give the FTC authority to prosecute companies for inadequate cybersecurity even in cases where the company's customers suffered no tangible injury.

The FTC's aggressive enforcement in this area is hardly surprising and, more importantly, appears to be here to stay. Indeed, while this article was being written, Equifax announced that it had fallen victim to a cyberattack of alarming size, which could impact potentially 143 million Americans (nearly half of the popula-

 ISSN 1559-3185

tion of the United States). And, sure enough, about a week after the hack occurred, the FTC announced that it had opened an investigation into the matter. Given the FTC's clear commitment to these data breach prosecutions, as well as the ever-increasing quantity of data collected in the digital economy, this article surveys the FTC's cybersecurity law landscape, proceeding in three parts. Part I examines the FTC's basis for such actions—Section 5 of the FTC Act, 15 U.S.C. § 45—and the hallmark cases that have been litigated under the statute. Part II discusses recent FTC enforcement actions and the resulting settlements. Part III addresses still-open legal questions and provides practice pointers—synthesized from recent settlement decisions—in order to help companies establish and enforce cybersecurity policies that pass muster under the FTC Act. Finally, we note that while the FTC has wide prosecutorial authority under Section 5 to pursue cases related to all kinds of Internet conduct, this article focuses exclusively on the FTC's actions in response to data breaches.

Part I: FTC Act Section 5's Applicability To Cybersecurity Prosecutions

Passed in 1914, and (most recently) substantively amended in 1994 and 2006, the FTC Act provides the legal authority the FTC has relied upon to prosecute cybersecurity cases. For the purposes of this article, we focus on two critical provisions of the Act—Section 5(a) and Section 5(n). Section 5(a) of the Act—often referred to as the consumer protection part of the statute—empowers the FTC to police ''***unfair*** or ***deceptive*** acts or practices in or affecting commerce.'' 15 U.S.C. § 45(a)(1). Section 5(n), added by Congress in 1994, further explains that conduct is ''***unfair***'' only when 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.'' 15 U.S.C. § 45(n) (emphasis added). For years, the FTC largely interpreted Section 5 through the lens of traditional antitrust and consumer protection law, using it to police conduct identified as anticompetitive or unfair. (False advertising, for example, is often prosecuted under Section 5.)

But in 2005, with the explosion of the Internet and the advent of big data, the FTC began to use Section 5 in a new way—prosecuting companies with allegedly deficient cybersecurity policies (or, in some cases, no cybersecurity policies at all) on the grounds that such conduct was ''deceptive'' or ''unfair'' to consumers. Because many of the FTC's early cybersecurity prosecutions resulted in settlements, the FTC's strategy went largely untested in the federal courts. In fact, only in 2015 did the Third Circuit issue its landmark decision in *FTC v. Wyndham Worldwide Corp.*, the first decision to analyze the FTC's authority to regulate cybersecurity. In many ways, *Wyndham Worldwide* has set the stage for the aggressive cybersecurity enforcement we see today.

The *Wyndham Worldwide* case began when, on three occasions in 2008 and 2009, hackers accessed Wyndham Worldwide Corporation's (''Wyndham'') computer systems and stole personal and financial information from over 600,000 Wyndham customers. Collectively, the hacks led to over $10.6 million in fraudulent charges and required the customers to spend time and money resolving the fraudulent charges and mitigating subsequent harm. In response to the hacks, the FTC sued, alleging that Wyndham's conduct—failing to adequately protect its customers' personal and financial information—amounted to an ''unfair'' practice under Section 5(a) of the FTC Act. Specifically, the FTC claimed that Wyndham, among other things, had (i) allowed hotels to store payment cards in clear readable text; (ii) used easily-guessed passwords for their property management systems; (iii) failed to use readily available security measures like firewalls or programs to detect and prevent unauthorized access to its systems; and (iv) failed to adopt appropriate incident response procedures (which may have prevented the later hacks given that the hackers used the same technical methods for each hack). *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240-41 (2d Cir. 2015). Wyndham moved to dismiss the complaint, arguing that Section 5(a)'s unfairness prong did not grant the FTC the authority to regulate cybersecurity-related conduct. The district court denied Wyndham's motion, and the Third Circuit granted interlocutory appeal on the question.

The Third Circuit likewise rejected Wyndham's argument, holding that the FTC has authority to regulate cybersecurity under Section 5(a)'s unfairness prong. The court concluded the FTC can prosecute unfairness claims based on cybersecurity-related conduct whenever, as required by Section 5(n), the challenged conduct causes consumers a substantial, unjustified injury that they could not have reasonably avoided. *Id.* at 245-47. Because the FTC's complaint demonstrated that Wyndham's customers had suffered such an injury, the Third Circuit allowed the case to proceed.

While *Wyndham Worldwide* was a victory for the FTC's cybersecurity agenda in that it supported the agency's authority to regulate cybersecurity conduct generally, recent developments indicate that the FTC's authority in such cases may be narrower than *Wyndham Worldwide* initially suggested. In June, for example, the Eleventh Circuit heard oral argument in another critical cybersecurity case, *LabMD, Inc. v. FTC*. LabMD was a clinical laboratory that operated from 2001 to 2014. In 2005, LabMD's billing manager downloaded a file sharing program called LimeWire on her work computer and, as a result of downloading the program, shared publicly much of the information on her computer. One of the shared files—the ''1718 file''—contained sensitive personal information for roughly 9,300 LabMD patients. In 2008, LabMD was approached by Tiversa Holding Company (''Tiversa''), a data security company that had downloaded the 1718 file as a business tactic in the hopes that LabMD would hire Tiversa to strengthen LabMD's cybersecurity policies. When LabMD refused to retain Tiversa, Tiversa shared the file with the FTC. The FTC then opened an administrative action alleging that LabMD's inadequate cybersecurity constituted ''unfair'' competition under Section 5 of the FTC Act and entered a Final Order requiring the company to implement several cybersecurity compliance measures.

LabMD appealed to the Eleventh Circuit and also sought to stay the FTC's order pending the results of its appeal. LabMD's argument was simple: unlike in *Wyndham Worldwide*, where customers' data was publicly

  WCR ISSN 1559-3185

hacked and then used to commit millions of dollars' worth of fraudulent transactions, the leak of LabMD's 1718 file did not cause—and was not likely to cause—substantial injury to consumers, as required under Section 5(n). Specifically, LabMD submitted that none of its customers had suffered any harm; none had fallen victim to identity theft or had their personal medical information stolen. The FTC disagreed, responding that the leak of ''the 1718 file was likely to cause substantial injury'' to LabMD's customers for two reasons. First, the FTC argued the phrase ''likely to cause'' in Section 5(n) need not mean ''probable''; instead, the FTC interpreted the language to cover cases raising ''significant risk,'' in which ''the potential injury is large, even if the likelihood of the injury occurring is low.'' *LabMD Inc. v. FTC*, 678 F. App'x 816, 820-21 (11th Cir. 2016). Second, as to whether the injury was ''substantial,'' the FTC argued it did not matter that none of LabMD's customers data was ever publicly disclosed; instead, it claimed that even ''purely conceptual'' harm—i.e., the harm that would have occurred had the data been publicly released—was sufficient to satisfy Section 5(n)'s ''substantial injury'' requirement. *Id.*

In November 2016, the Eleventh Circuit granted LabMD's request for a stay. In its opinion, the court viewed the FTC's interpretation of Section 5(n)'s ''likely to cause'' and ''substantial injury'' language with skepticism, acknowledging that the proposed interpretation raised ''a serious legal question.'' *Id.* On June 21, 2017, during oral argument on the merits of the case, the court again called into question the FTC's position. Indeed, as Judge Tjoflat observed when commenting on the alleged injury to LabMD customers: ''A tree fell and nobody heard it—that's the kind of case we have here.'' Oral Argument at 16:00-16:06, *LabMD Inc. v. FTC*, No. 16-16270 (11th Cir. June 21, 2017).

Equally instructive, the Eleventh Circuit also expressed doubts about the merits of the FTC's case during oral argument, questioning whether it made sense to use the agency's proposed ''reasonableness'' standard in these data security cases. In this respect, the Court suggested that using a ''reasonableness'' standard may be insufficiently vague, calling it as ''nebulous as you can get'' in that it fails to provide businesses fair notice as to the type of conduct that violates the statute. *Id.* at 22:52-22:56. In fact, the Court went so far as to say that a reasonableness standard could result in serious hindsight bias, and that it may not be a good public policy objective for the FTC to have an ''unlimited license to find out what is reasonable and is unreasonable in the economy.'' *Id.* at 31:09-31:27. In response, the FTC conceded that a reasonableness standard would create an ever-shifting target for compliance, but still insisted that businesses could comply with the standard (and in fact do so routinely in tort law) and that Congress intended to adopt a reasonableness standard in passing the FTC Act.

Given the Eleventh Circuit's initial reactions to the FTC's position, both in its stay opinion and during oral argument, a final decision in *LabMD* should provide more clarity. The Eleventh Circuit should provide guidance on what type of consumer injury is required under Section 5 and, in so doing, could meaningfully restrict the FTC's authority to initiate cybersecurity prosecutions going forward.

Part II: The FTC's Prosecutions Of (and Settlements With) Uber and Ashley Madison

Despite the Eleventh Circuit's initial skepticism over the FTC's approach in *LabMD*, the agency continues to aggressively prosecute and settle cybersecurity cases under Section 5. The most recent example, as mentioned earlier, is the FTC's August 2017 settlement with Uber flowing from a data breach in 2014. This section provides a brief overview of the Uber settlement as well as one other recent settlement—the FTC's settlement with website Ashley Madison, secured at the end of 2016. In particular, it focuses on the relief won by the FTC in those cases, explaining the compliance policies and procedures that Uber and Ashley Madison agreed to as part of the settlements.

Uber In 2014, hackers breached Uber's servers and were able to access a file that contained sensitive personal information of Uber drivers, including some drivers' names, driver licenses, bank account and routing numbers, and social security numbers. Prior to the hack, Uber had repeatedly assured its customers—both its drivers and riders—that their personal information was secure. For example, Uber's privacy policy promised its customers that Uber used ''standard, industry-wide, commercially reasonable security practices'' in order to safeguard their data. Complaint at 16, *Uber Techs., Inc.*, No. 1523054 (F.T.C. Aug. 15, 2017), https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_complaint.pdf. Uber's customer service representatives likewise made similar statements to customers, assuring them that Uber used ''the most up to date technology and services,'' was ''extra vigilant in protecting all private and personal information,'' and kept customers' information ''secure and encrypted to the highest security standards available.'' *Id.* at 17.

During its investigation into the Uber data breach, the FTC learned that the breach began when an intruder accessed Uber's cloud-based storage platform—the Amazon S3 Datastore provided by Amazon Web Services. The FTC traced the breach back to an Uber engineer who had publicly posted to GitHub, a code-sharing website used by software developers, an access key that granted full administrative privileges to all data and documents stored on Uber's Amazon S3 Datastore. The FTC found that Uber could have adopted a number of practices that may have prevented the breach; specifically, the FTC found that Uber had (i) failed to require programmers and engineers accessing the Amazon S3 Datastore to use distinct access keys for distinct portions of the database, instead permitting all programmers and engineers to use a single access key that provided full administrative privileges over all data within the Amazon S3 Datastore; (ii) failed to restrict access to systems based on employees' job functions; and (iii) failed to require a more developed, multi-factor authentication process for granting access to its Amazon S3 Datastore. *Id.* at 18. The FTC also learned that the file was both unencrypted and stored in fully readable text, making it significantly easier for the hacker to access the data in usable form. Given these cybersecurity missteps, the FTC alleged that Uber's prior representations about the robustness of its cybersecurity practices were ''false or misleading.''

In addition to the 2014 data breach, the FTC also took issue with Uber's public statements, in which Uber claimed to actively monitor users' personal information. For example, in a November 18, 2014 announcement responding to customer concerns about data security, Uber stated that '' access to rider and driver accounts is being closely monitored and audited by data security specialists on an ongoing basis.'' *Id*. at 11. According to the FTC, Uber did not live up to this promise because, although Uber had set up an automated system to deal with user data concerns, it ''did not timely follow up on automated alerts concerning the potential misuse of consumer personal information.'' *Id*. at 13. Moreover, the FTC alleged that Uber failed to monitor internal access to personal information unless an employee specifically reported that a co-worker had inappropriately accessed a user's data. As with the data breach, the FTC alleged that Uber's statements were ''false or misleading'' because they did not accurately reflect the on-the-ground reality of Uber's cybersecurity practices.

Uber settled with the FTC in August 2017, agreeing to two critical conditions. First, Uber agreed not to misrepresent the extent to which it:

(i) monitors internal access to consumer's personal information, or

)ii) protects the privacy, confidentiality, security, or integrity of such information.

Second, and more interestingly, Uber agreed to establish and implement a ''Mandated Privacy Program'' in order to protect the confidentiality of consumers' personal information and to study and address any privacy risks related to development of new or existing Uber services. Notably, the settlement agreement contained important procedural requirements, particularly in relation to the Mandatory Privacy Program. For example, Uber must make periodic compliance reports, sworn under penalty of perjury, to the FTC and must obtain written assessments of the Mandatory Privacy Program from a qualified, objective, and independent third-party.

Ashley Madison By way of background, Ashley Madison is a website designed to connect married individuals seeking to have extra-marital affairs. It is owned by Ruby Corp. (''Ruby''), which also owns and operates other dating websites like CougarLife.com, Established-Men.com, and ManCrunch.com. The FTC's prosecution of Ruby and Ashley Madison began on July 12, 2015, when Ashley Madison employees first noticed that a large data file was being transferred from one database to another. Sure enough, a notice appeared on Ashley Madison's servers the following day, stating that the company had been hacked, demanding immediate shut down of AshleyMadison.com, and warning that refusal to do so would lead to the release of all customer records for the sites.

On August 18 and 20, 2015, the hackers did precisely that, leaking 9.7 gigabytes of information pertaining to more than 36 million Ashley Madison customers. In many ways, the FTC's prosecution of Ashley Madison was strikingly similar to its prosecution of Uber. For example, the FTC likewise seized on Ashley Madison's public statements touting the strength of its cybersecurity, including statements that the site was ''100% secure,'' ''risk free,'' ''completely anonymous,'' and the site's portrayal of a ''Trusted Security Award'' icon that claimed the site was an ''SSL Secure Site.'' Complaint at 30, *FTC v. Ruby Corp*., No. 1:16-cv-02438 (D.D.C. Dec. 14, 2016), ECF No. 1. And just as it did with Uber, the FTC claimed that these representations were ''false and misleading'' because, in reality, Ashley Madison was doing far less to protect its customers' data. Indeed, the FTC identified a host of practices that undermined Ashley Madison's security-related claims; specifically, the FTC took issue with Ashley Madison's failure to:

(i) have a written information security policy;

(ii) implement reasonable access controls, such as revoking passwords for ex-employees, regularly monitoring unsuccessful login attempts, or restricting access to systems based on employees' job functions;

(iii) adequately train personnel to perform data security-related duties; (iv) engage third-party service providers to implement reasonable security; and

(iv) monitor activity on the Ashley Madison systems and servers. *Id*. at 31.

The FTC also targeted Ashley Madison for failing to delete the accounts of those customers who paid for Ashley Madison's ''Full Delete'' service, an offering through which Ashley Madison customers purportedly could pay the company to delete all the personal information associated with their accounts.

Ashley Madison eventually decided to settle with the FTC, and the settlement it reached strongly resembled the one the FTC just entered with Uber. Indeed, Ashley Madison likewise agreed not to make any false or misleading representations regarding the extent of its cybersecurity policies, and to implement a Mandatory Data Security Program. But for all the similarities between the Uber and Ashley Madison actions and settlements, there were two noticeable differences. First, the FTC obtained monetary relief from Ashley Madison, securing a judgment of $8.75 million. (The FTC suspended part of the judgment because of Ashley Madison's financial condition, agreeing to collect $825,500 from Ashley Madison but preserving the right to collect the remaining balance should it become clear that Ashley Madison misrepresented its financial condition.) Second, in addition to alleging that Ashley Madison's cybersecurity practices were deceptive, the FTC also claimed that the company's failure to take reasonable steps to protect customer information constituted an ''unfair'' practice under Section 5(a) of the FTC Act.

Part III: Open Legal Questions and Practice Pointers

Because the FTC's prosecution of cybersecurity cases is a relatively new phenomenon, a number of legal questions remain open in such cases. At a threshold level, for example, there is the question of whether and to what extent the FTC can prosecute data security cases that do not involve misrepresentations about a company's cybersecurity protocols. The easiest cases for the FTC to prosecute are those involving affirmative misrepresentations about the steps a company has taken to protect user data, which allow the FTC to use a more traditional deception-based theory under Section 5. Conversely, for unfairness-based actions, there is significantly more uncertainty about how the FTC can prove a violation of the FTC Act. Specifically, it remains

  WCR ISSN 1559-3185

unclear (i) what type of customer injury is required before the FTC can initiate an enforcement action, and (ii) what legal standard will be used to evaluate the lawfulness of the defendant's cybersecurity practices.

Nonetheless, a few must-follow principles have emerged from the FTC's recent prosecutions. Along those lines, we include below a list of practice pointers intended to help businesses adopt and enforce cybersecurity policies that pass muster under Section 5 of the FTC Act.

■ **Adopt a written cybersecurity policy:** Businesses should make sure they adopt—and actively enforce—a comprehensive cybersecurity policy covering customers personal information. In adopting its policy, the business should make sure the requisite divisions are communicating about the scope and nature of the policy—i.e., the information technology department engages with the marketing and/or compliance departments—to make sure any public statements or customer-facing communications accurately describe ongoing efforts and underlying technology used to protect customers information.

■ **Train employees on cybersecurity issues:** Businesses should train their employees on cybersecurity issues, including the methods to protect information and the serious damage that security breaches may cause. In particular, businesses should make sure their information technology departments have a working knowledge of cybersecurity technology and remain informed of industry and technological developments.

■ **Establish separate servers and implementreasonable firewalls betweenservers and employees:** Businesses should refrain from hosting all customer information in one location—i.e., on one server. Instead, individual divisions or projects within the company should have their own server or system. Likewise, businesses should restrict access to servers/systems based on employees' job titles and professional responsibilities. Only those employees whose job responsibilities require access to customer information should be granted access, and protocols should be established to ensure that employees access is terminated if they leave the company or otherwise no longer require access.

■ **Restrict employees' administrative (e.g., download) rights:** Businesses should restrict employees' administrative access rights, particularly when it comes to downloading external software. Indeed, during the oral argument in *LabMD*, the FTC specifically criticized LabMD for allowing its employees to have administrative rights and the ability to download programs, including the file-sharing program that caused the data breach in that case. Oral Argument at 27:00-27:45, *LabMD, Inc. v. FTC*, No. 16-16270 (11th Cir. June 21, 2017).

■ **Use multi-factor authentication:** Multi-factor authentication is a type of access control in which a user is granted access to a system (or server) only after she presents several independent pieces of evidence. For example, some systems require the user to type in a password and then, after the password has been verified, enter a new code that is sent to the user via e-mail or text message. In short, multi-factor authentication sets up numerous security checkpoints, all of which must be successfully ''passed'' in order to gain access to the system. Although the FTC only ***suggested*** in 2015 that multi-factor authentication should be used to protect customer information, *see* Fed. Trade Comm'n, *Start with Security: A Guide for Business– Lessons Learned from FTC Cases* at 5 (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (''Businesses also may want to consider other protections – two-factor authentication, for example – that can help protect against password compromises.''), it now seems that FTC is beginning to require multi-factor authentication to comply with Section 5. (Indeed, the failure to adopt multi-factor authentication procedures was a focal point in both the Ashley Madison and Uber prosecutions.)

■ **Monitor servers containing customer information and actively pursue potentially suspicious activity:** Businesses should adopt a methodology to monitor (i) who is accessing their customers' information, (ii) from where it is being accessed, (iii) when it is being accessed, and (iv) whether the access appears to be unauthorized. And the monitoring should apply to both external individuals and internal employees. Equally important, businesses must actively investigate seemingly suspicious incidents (e.g., failed log-in attempts).

■ **Engage third-party vendors where appropriate:** Businesses should engage third-party vendors with relevant subject matter expertise where appropriate. In particular, businesses can retain third-party to ''test'' existing security measures or, for those businesses with less developed capabilities, retain experts to assist in developing and implementing their cybersecurity program.

Importantly, while these are some strategies to help businesses establish robust cybersecurity policies, they are by no means exhaustive. Indeed, given how fast the digital world and the cybersecurity landscape change, businesses should remain abreast of critical technological and legal developments in this area.