PUBLICATION

Lessons Learned from LabMD's Successful Challenge to the FTC's Cyber Authority and Wyndham's Monumental Settlement with the FTC

Authors: Samuel Lanier Felker
January 08, 2016

On the shifting sands of cyber security regulation, it is important to understand the outcome of two recent enforcement cases brought by the Federal Trade Commission (FTC) – one against clinical lab services company LabMD, Inc. and the other against international hotel giant Wyndham. In the former case, LabMD was accused of security breaches that allegedly exposed its patients' private information, but on November 19, 2015, an administrative law judge dismissed the FTC's case against LabMD on the merits, finding the FTC failed to carry its burden of proof under Section 5 of the Federal Trade Commission Act (FTC Act) that LabMD's security failures caused, or were likely to cause, substantial injury to consumers. Although the FTC has appealed, this represents a successful and serious challenge to the FTC's authority to regulate cyber security breaches, particularly in cases where there is no demonstrated "injury" from the data breach.

On the other hand, the long and contentious case against Wyndham Hotels and Resorts, LLC (Wyndham) and certain of its affiliates ended in settlement with the FTC after the Third Circuit upheld the FTC's statutory authority to regulate and enforce cyber security breaches. The Wyndham settlement, announced December 9, 2015, provides insight into what the FTC considers reasonable data security, particularly when subsidiaries and franchisees are involved.

We will discuss both cases and then provide important "takeaways" for companies to consider in developing their cyber security procedures.

Dismissal of the FTC's Case Against LabMD

In the August 28, 2013, complaint, the FTC charged that because of two security incidents, LabMD, a clinical testing laboratory, failed to provide reasonable and appropriate security measures for personal information and this conduct caused or was likely to cause substantial injury to consumers. The FTC alleged that LabMD was liable for "unfair" acts or practices under Section 5 of the FTC Act, thereby exposing personal information of up to 10,000 customers to hackers in two separate incidents in 2009 and 2012.

Section 5 of the FTC Act (15 U.S.C. § 45(n)) states that the FTC "shall have no authority to declare unlawful an act or practice on the grounds that such act or practice is unfair unless [1] the act or practice 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."

However, the administrative law judge found that the FTC failed to establish an unfair trade practice because the FTC failed to prove the first prong of the three-part test above – that the alleged unreasonable conduct caused or was likely to cause substantial injury to consumers. Specifically, the evidence failed to prove that the limited exposure of the data resulted, or was likely to result, in any identity theft-related harm. The evidence also failed to prove that embarrassment or similar emotional harm likely to be suffered from the exposure is a "substantial injury" where there is no proof of other tangible injury. Lastly, the theory that the company's data is "at risk" of a future data breach was also rejected. In rendering the decision, the administrative law judge stated,

To impose liability for unfair conduct under Section 5(a) of the FTC Act, where there is no proof of actual injury to any consumer, based only on an unspecified and theoretical "risk" of a future data breach and identity theft injury, would require unacceptable speculation and would vitiate the statutory requirement of "likely" substantial consumer injury. At 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.

Accordingly, the complaint was dismissed. The FTC promptly appealed the decision to the commissioners of the FTC without specifying any new grounds. Click here to see the pleadings in the LabMD – FTC case.

The Wyndham Settlement

Several years ago, Wyndham was the victim of sophisticated cyberattacks by criminal hackers, who accessed customer information at certain Wyndham Hotels and Resorts-brand hotel properties. Wyndham promptly alerted law enforcement agencies, retained computer forensic experts, implemented significant security enhancements and assisted franchised Wyndham Hotels and Resorts-brand hotels in reinforcing their information security. Wyndham also made prompt efforts to notify the hotel customers whose information may have been compromised, and offered them credit monitoring services.

After an investigation, the FTC filed a complaint alleging violations of Section 5 of the FTC Act, 15 U.S.C. § 45, which bars "unfair or deceptive acts or practices in or affecting commerce." The FTC essentially argued that hackers had gained access to the network of a Wyndham franchisee and then exploited security on the hotel chain's corporate network to steal credit card information from customers of other Wyndham franchisees.

In the past decade, the FTC had brought more than 40 such enforcement actions against companies alleging data security violations. In each of those actions, the defendant entered into a settlement agreement (consent decree) with the FTC rather than litigating the claims. However, Wyndham took a novel and aggressive approach, defending on the basis that the FTC had no authority to "impose general data-security standards" upon businesses in all industries in the absence of specific legislation. Earlier this year, the Third Circuit decided otherwise and confirmed the FTC's statutory authority to regulate cyber security practices under the unfairness prong of Section 5 of the FTC Act by bringing lawsuits against companies over data security practices the FTC deems unreasonable.

Following are the key terms of the settlement between Wyndham and the FTC:

- Wyndham will not pay any monetary relief.
- The company is granted a Safe Harbor if it continues to meet certain requirements for "reasonable information security" outlined in the FTC's consent order.
- The consent order applies only to payment card information, and does not apply to any other categories of personally identifiable information. Payment Card Industry (PCI) certification will satisfy Wyndham's reporting requirement and provide the basis for the Safe Harbor.
- The duration of Wyndham's obligations under the consent order will in no event be longer than 20 years, and in several areas will be shorter.

Wyndham issued the following statement:

We are pleased to reach this settlement with the FTC, which does not hold Wyndham liable for any violations, nor require Wyndham to pay any monetary relief. We chose to defend against this litigation based on our strong belief that we have had reasonable data security in place, and that the FTC's position could have had a

negative impact on the franchise business model. This settlement resolves these issues, and sets a standard for what the government considers reasonable data security of payment card information. Safeguarding personal information remains a top priority for our company at a time when companies and government agencies are increasingly the targets of cyberattacks.

Click here to see the pleadings in the Wyndham – FTC case.

Key Takeaways

Would-be breach defendants and data owners and processors everywhere should consider the following takeaways.

(1) For now, it will be substantially more difficult for the FTC to act arbitrarily in cases in which no actual harm can be shown. The enforcement requirements set forth by the administrative law judge in the LabMD case parallel the same type of pleading and proof of injury standards that private litigants have had to meet in connection with the majority of data breach cases that have been decided. In order to be liable under Section 5 of the FTC Act for failing to maintain "reasonable and appropriate" security for personal information, the data breach must have "caused or be likely to cause" actual and substantial consumer injury – which has now been interpreted to mean that emotional harm or an increased risk that hypothetical or theoretical harm is not enough. The standard to which FTC was held is much like the "actual injury" constitutional standing requirements that have plagued plaintiffs in civil breach litigation cases.

(2) Defendants currently in the FTC's crosshairs may find themselves with better settlement bargaining power. The FTC has secured numerous settlements and consent decrees (53 of 55 data security cases) by asserting that the company's failure to protect personal information, alone, was sufficient to establish the "substantial injury" required by Section 5. Following the LabMD ruling, at least for now, companies will be in a much stronger bargaining position where there is no actual injury to customers or others as a result of a data breach. In the past, the FTC acted as though it had total latitude to bring actions in the absence of likely harm, but this decision changes that dynamic as more enforcement targets may challenge the FTC's authority. Further, the Wyndham settlement's focus solely on credit card data, and not globally on other forms of personally identifiable information, indicates that Wyndham had the upper hand in negotiations in several respects.

(3) The FTC's authority to bring enforcement actions against alleged "violators" may not reach as far as the Office for Civil Rights (OCR) authority over health care companies and their business associates. When a complaint or breach of unsecured protected health information is investigated by OCR, the case is assessed based on strict compliance with the applicable HIPAA Privacy, Security and/or Breach Notification Rules. OCR need not prove actual, or potential, harm to attempt to levy large penalties. In contrast, should the administrative law judge's decision in the LabMD case stand, the FTC will now have to demonstrate actual or probable harm to consumers – perhaps significantly limiting the FTC's enforcement capabilities. If the FTC is not successful in overturning the LabMD decision, the FTC could potentially attempt to implement its own regulations in an effort to permit easier enforcement.

(4) The FTC for the first time provided valuable guidance about what it views as reasonable cyber security procedures to protect credit card information, particularly where there are franchisees and affiliates involved. Rather than addressing Wyndham's comprehensive data security program, the Consent Order specifically notes safeguards that should be utilized to protect against theft of payment card information. The settlement incorporates the PCI DSS as the applicable standard to be applied in the ongoing audits of Wyndham. By adopting this payment card industry standard, the FTC provided valuable insight into the procedures that it deems reasonable related to credit card data. The settlement also mandated certain firewall

procedures between the company's servers and its franchisees, also required by PCI DSS, which is instructive as to what the FTC expects of any company dealing with third parties.

Looking Ahead

As mentioned, the FTC has already appealed the administrative law judge's ruling in the LabMD case, and in addition, numerous lawsuits have been filed related to the case. There is parallel litigation ongoing between LabMD and cyber security firm Tiversa Holding Corp., with the latter accused of stealing LabMD's confidential customer records and leaking them to the FTC when LabMD did not hire Tiversa to remediate the alleged breach. Tiversa in turn has sued LabMD and its CEO for defamation for accusing the company of hacking and the alleged extortion scheme. In yet another proceeding, LabMD has sued the agency lawyers for costs, saying it was ruined by an illegal and unethical prosecution.

Now that the FTC's case against Wyndham is resolved, it is important to observe the FTC's enforcement activities regarding theft of credit card information to see if the guidelines provided in the settlement will be applied in other cases. For example, only one week after the Wyndham settlement, the FTC announced a $100 million settlement with LifeLock, Inc. resolving allegations that LifeLock's advertising and data security practices violated a 2010 court order prohibiting it from misrepresenting its identity theft protection services and requiring it to establish and maintain a comprehensive information security program. In its press release, the FTC commented that PCI DSS certification is insufficient in and of itself to establish the existence of reasonable security protections, noting that the Wyndham order calls for a number of additional significant protections, including the implementation of risk assessments, certification of untrusted networks and certification of the assessor's independence and freedom from conflicts of interest. In its press release, the FTC cautioned, "As we have long emphasized, the reasonableness of security will depend on the facts and circumstances of each case."

Baker Donelson's privacy and security team will continue to monitor what is expected to be a lengthy appeal process for LabMD and report on other notable legal developments. Despite the recent FTC setback in LabMD, we still believe that once a company becomes an FTC target, it is unlikely to give up without a fight. Therefore, it is important for businesses with consumer data (including patient data and credit card information) to work with attorneys and IT consultants to implement reasonable and appropriate privacy and security measures to reflect lessons learned from the FTC's regulatory activities, and to prepare for future breaches.

For more information about how this ruling may affect your business or for assistance with your litigation, compliance or breach preparedness and response needs, contact any member of the Firm's Privacy and Information Security Team.