Reading the Section 5(a) Tea Leaves: What the end of 2015 may suggest about the FTC priorities in 2016

Breana Chea Jeter
01.2016

The end of 2015 represented a mixed bag for the Federal Trade Commission on privacy enforcement. In November, the FTC's Chief Administrative Law Judge dismissed the FTC's complaint against LabMD for a possible data breach of 1,718 patients' insurance claim information. The patient's sensitive information was discovered on peer-to-peer software by a data security company seeking to sell its services to LabMD. While LabMD maintained that the patient's information never left the company's network and that there was no actual breach, the FTC proceeded with its lawsuit on the grounds that LabMD's security practices were so unreasonable as to likely cause substantial consumer harm. The ALJ, however sided with LabMD, dismissing the complaint because there was no evidence of consumer harm, only speculation by the FTC that an unspecified harm may occur in the future. The ALJ rejected the FTC's argument that liability can be imposed based solely on the risk of data breach; according to the ALJ, "[f]undamental fairness dictates that proof of likely substantial consumer injury under Section 5(a) requires proof of something more than an unspecified and hypothetical 'risk' of future harm, as has been submitted in this case." The FTC is appealing the decision.

In December, however, Wyndham Hotels and Resorts agreed to settle the FTC's enforcement action, which alleged that Wyndham's inadequate data security measures "unfairly" exposed consumer's payment card information to three separate data breaches between 2008 and 2010. We previously wrote about the enforcement action here. As a refresher, in Wyndham the FTC relied on Section 5(a) of the FTC Act as its authority for enforcement actions; the statute provides that "unfair or deceptive acts or practices in or affecting commerce…are…declared unlawful." According to the FTC, Wyndham's deficient security practices, including the failure to use readily available security measures such as firewalls and encryption, allegedly caused "the compromise of more than 619,000 consumer payment card account numbers, the exportation of many of those account numbers to a domain registered in Russia, fraudulent charges on many consumers' accounts, and more than $10.6 million in fraud loss." Although Wyndham made valiant attempts at challenging the FTC's authority to enforce data security breaches under Section 5(a), the District of NJ and the Third Circuit disagreed and allowed the lawsuit to proceed. In that sense, the Wyndham case represents a tremendous victory for the FTC. As Chairwoman Edith Ramirez proclaimed after the entry of the settlement, "This settlement marks the end of a significant case in the FTC's efforts to protect consumers from the harm caused by unreasonable data security. Not only will it provide important protection to consumers, but the court rulings in the case have affirmed the vital role the FTC plays in this important area."

The dismissal of the LabMD matter on the other hand may represent a figurative bee in the Chairwoman's bonnet, particularly with respect to consumer harm. In reality, the facts of LabMD differ starkly enough in comparison to the facts of Wyndham, where a massive breach resulted in over 10 billion in fraudulent charges on many consumer's accounts. Nevertheless, the LabMD decision is significant because it appears to place a higher burden on the FTC to prevail in unfairness claims.

Regardless, companies should not expect the FTC to discontinue its vigilant efforts under Section 5 of the FTC Act against companies with inadequate data security measures, and should not expect leniency for failure to adhere to those standards. While the LabMD dismissal should make companies more bullish in negotiating with the FTC in cases where there is no actual harm to consumers, at the end of the day, 2016 does not appear to be the year in which the FTC will slow down its pursuit of companies with data security failures that lead to consumer data breaches. Commissioner Julie Brill's comments at PrivacyCon last Thursday (see DataPoints post here) shows that, if anything, the FTC expects companies to ensure that their data security measures keep up with new and changing technologies.