COVINGTON

COVINGTON & BURLING LLP

E-ALERT | Privacy & Data Security

April 11, 2014

BREAKING DOWN THE COURT'S DECISION IN *FTC V. WYNDHAM WORLDWIDE CORP.*

Earlier this week, in a much-anticipated decision, Judge Esther Salas of the District of New Jersey denied Wyndham Hotels and Resorts' motion to dismiss a Federal Trade Commission ("FTC") lawsuit alleging Wyndham violated the FTC Act's prohibition against "unfair practices" by failing to provide "reasonable" security for the personal information of its customers. Although the FTC has settled complaints relying on this broad interpretation of its unfairness authority, this is the first time a court has had the opportunity to weigh in on the scope of that authority in the privacy and data security context. Judge Salas rejected each of Wyndham's challenges to the FTC's authority and to the sufficiency of the complaint in this case. The FTC's suit against Wyndham will therefore proceed.

This alert provides a detailed look at the parties' arguments and the court's holdings in order to assess what it means for businesses going forward. The significance of the decision can be summed up in four points:

- **The FTC's unfairness authority in the data-security context survives—for now.** The court held that the FTC has the authority under the FTC Act to take action against companies that fail to provide reasonable security for the personal information they maintain. Although the court's thinking on this point is unlikely to change at a later stage of the litigation, Wyndham could seek permission to immediately appeal the decision to the Court of Appeals for the Third Circuit or wait until final judgment, when it would have the right to appeal. Because this is an issue of statutory interpretation, the Third Circuit would take a fresh look at Wyndham's arguments.
- **The court endorsed the FTC's practice of exercising its unfairness authority through adjudicative proceedings rather than rulemakings.** The court rejected Wyndham's argument that the FTC may not proceed on a case-by-case basis against companies alleged not to have provided reasonable security for personal information, but rather must establish data-security rules in advance. The court held that the FTC's reasonableness standard, which it has articulated and developed in guidance, consent orders, and draft complaints, provides companies with fair notice of what is "unfair" in the data-security context.
- **The FTC's complaint was found to contain sufficient allegations of unfairness and deception—but these allegations will need to be supported by evidence.** The court decided a motion to dismiss under Federal Rule of Civil Procedure 12(b)(6). This means the court only could look to the allegations in the FTC's complaint in deciding whether the FTC had stated plausible unfairness and deception claims against Wyndham. Moreover, the court had to accept the facts the FTC alleged as true. Later in the case, the FTC will have to produce evidence to support its claims, which is a much taller order.
- **The FTC's data-security authority is still in jeopardy.** Although the FTC is the plaintiff in this case, it is really Wyndham that is on the offensive. If Wyndham prevails in the court of appeals on the issue of the FTC's statutory authority or the need for rulemaking, it would be a major blow to the agency's ability to pursue companies for lax data-security practices. Wyndham could also prevail

in the district court if the FTC fails to produce sufficient evidence in support of its claims to survive a motion for summary judgment, a result that could be nearly as devastating to the FTC as a loss in the court of appeal. On the other hand, if the FTC manages to win in the district court and the court of appeals, the victory will simply ensure that the agency can continue doing what it has been doing for years: using its unfairness authority to regulate data-security practices.

THE FTC'S SUIT AGAINST WYNDHAM

In June 2012, the FTC announced it had filed a complaint against Wyndham "for alleged data security failures that led to three data breaches at Wyndham hotels in less than two years."[1] The complaint alleged that Wyndham had engaged in (1) deceptive practices because its privacy policy misrepresented the measures it took to protect consumers' personal information and (2) unfair practices because its failure to safeguard personal information caused "substantial consumer injury."[2]

The announcement marked the first time a company facing allegations of unfairness or deception in the privacy and data-security context had refused to settle with the FTC. Before Wyndham, dozens of companies pursued by the FTC for privacy or data security infractions in violation of the FTC Act had chosen to settle with the agency rather than contest the agency's allegations in the Commission itself or in federal court. The settlements resulted in a line of consent orders (i.e., settlement agreements between the FTC and a company or individual) and draft complaints that were publicized along with the consent orders that some have called a "common law" of consent orders.

WYNDHAM'S ARGUMENTS AND THE COURT'S HOLDINGS

Wyndham's motion asked the court to dismiss the FTC's unfairness and deception claims. Wyndham's challenge to the unfairness claim has received the most attention from commentators because Wyndham argued that the FTC does not have the legal authority to bring unfairness claims against companies for failing to provide reasonable data security. Wyndham also argued that, even assuming the FTC possesses this authority as a general matter, the agency had failed to plausibly allege unfairness—or deception—in this case.

The Scope of the FTC's Unfairness Authority

Wyndham argued that the FTC's authority to prevent unfair practices does not enable it to pursue companies for alleged failure to maintain "reasonable" data-security practices. Wyndham contended that the broad grant of authority in Section 5 of the FTC Act to prevent "unfair or deceptive acts or practices" must be read in conjunction with the many specific laws that give the FTC authority to prescribe data-security rules for and take action against companies that fail to provide reasonable security for the data they maintain. Wyndham argued that sector- and information-specific laws (such as the Fair Credit Reporting Act) that explicitly give the FTC authority to regulate data-security practices would be superfluous if the FTC Act already gave the agency that power. Moreover,

---

[1] FTC Files Complaint Against Wyndham Hotels For Failure to Protect Consumers' Personal Information (June 26, 2012), http://www.ftc.gov/news-events/press-releases/2012/06/ftc-files-complaint-against-wyndham-hotels-failure-protect.

[2] Section 5 empowers the FTC to "prevent . . . unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a)(2). Deceptive acts or practices are those that involve misrepresentations or omissions likely to mislead consumers acting reasonably under the circumstances to their detriment. FTC, Policy Statement on Deception (Oct. 14, 1983), http://www.ftc.gov/bcp/policystmt/ad-decept.htm. Unfair acts or practices are those that cause substantial consumer injury, not outweighed by countervailing benefits to consumers or competition, and that consumers could not reasonably have avoided. 15 U.S.C. § 45(n).

Wyndham noted, the FTC itself had on several occasions disclaimed authority to regulate data security under Section 5's unfairness prong.

The court rejected both arguments, noting that the sector- and information-specific laws merely "grant[ed] the FTC additional enforcement tools" that supplemented the agency's powers under Section 5. The court noted that statutes like the Fair Credit Reporting Act set forth different (and perhaps less strenuous) standards for proving injury than Section 5's requirement of a "substantial injury" not reasonably avoidable by consumers and not outweighed by countervailing benefits to consumers. The court also downplayed the significance of the FTC's previous statements regarding its unfairness authority in the data-security context, concluding that none had amounted to a "resolute, unequivocal position . . . that the FTC has no authority to bring any unfairness claim involving data security."

Fair Notice of Prohibited Conduct

A related argument Wyndham made was that the FTC could not exercise its Section 5 unfairness authority against companies that fail to provide "reasonable" security because it has not provided companies with notice of what reasonable security is. Instead of providing clear standards in the form of rules or guidance, the agency has indicated its expectations for companies only in draft complaints published together with consent orders that are the result of negotiations with individual companies. Without more advance guidance from the FTC, Wyndham argued, a lawsuit under Section 5's unfairness prong violates the Constitution's guarantee of due process, among other legal standards.

The court rejected this argument. The court construed Wyndham's motion as arguing that the FTC must promulgate rules requiring specific data-security practices before it can take action against companies for data-security failures. In rejecting this argument, the court noted that the FTC could proceed through case-by-case adjudications based on the "reasonableness" standard, which, the court seemed to suggest, gives companies sufficient notice about what the agency expects. The court also appeared to hold that the FTC's "public complaints and consent agreements" provided the fair notice Wyndham argued was lacking.

Sufficiency of the Allegations in this Case

Wyndham also argued that even assuming the FTC may bring Section 5 unfairness claims in some cases involving data-security issues, the agency's complaint in this case nonetheless fails because it does not contain factual allegations that state a plausible claim for relief. It also argued that the FTC's deception claim fails for similar reasons.

Unfairness Claim

An unfair practice is one that causes substantial consumer injury, not outweighed by countervailing benefits to consumers or competition, and that consumers could not reasonably have avoided. Wyndham's motion focused primarily on the nature of the injury alleged in the FTC's complaint—i.e., injuries alleged to have arisen after payment-card data was stolen in the breaches Wyndham suffered. The complaint alleged that millions of dollars of fraud was directly attributable to these breaches. Wyndham's motion noted that, even if these allegations of fraud are true, the allegations still do not mean that consumers suffered substantial injuries that were not reasonably avoidable. This is because federal law limits the amount for which a person can be liable when unauthorized charges are made on a payment card.

Wyndham also argued that the complaint did not sufficiently allege that any data-security failures *caused* the consumer injuries in this case. Wyndham's motion noted that the complaint "contains no factual allegations showing how the alleged data-security failures caused the intrusions, or how the intrusions resulted in any particular consumer harm."

Nonetheless, the court held that based on the factual allegations in the complaint—which it must accept as true at this stage of the case—the FTC had stated a plausible unfairness claim. The court pointed out that the complaint had alleged that "at least some consumers suffered financial injury that included 'unreimbursed financial injury'" and that it was reasonable to infer that Wyndham's "data-security practices *caused* theft of personal data, which ultimately *caused* substantial injury to consumers." As to whether the opportunity to be reimbursed by the card issuer meant that any injury was reasonably avoidable by the consumer, the court held that it could not "make such a far-reaching conclusion regarding an issue that seems fact dependent." In other words, this issue may have to await summary judgment.

Deception Claim

The FTC's complaint also alleged that Wyndham violated Section 5's deception prohibition by representing in its privacy policy that it had implemented reasonable security measures to protect personal information and then failing to do so. Wyndham argued, among other things, that Wyndham-branded hotels (most of which are franchises) are legally separate entities, and that the Wyndham corporate privacy policy excludes these entities from coverage. According to Wyndham, the privacy policy does not make representations about the entities that (it says) actually were affected by the breaches: the individual hotels.

The court rejected this argument, noting that the FTC's complaint had alleged that Wyndham itself (and not just its franchisees) had failed to employ reasonable security measures. The court also explained that a reasonable consumer reading the corporate privacy policy could understand the policy to make statements about the security of information at Wyndham *and* its franchisees, at least where Wyndham controls the information maintained by a franchisee. The court found these allegations to be sufficient to state a plausible claim for deception.

WHAT THE DECISION MEANS FOR BUSINESSES

The court's decision already has been hailed as a "landmark," and numerous commentators have described it as affirming the FTC's role as the United States' data protection authority. Many of these reactions do not take into account the context of the larger litigation between the FTC and Wyndham, which (despite having been pending for nearly two years) is still in its very early stages. Although the court's holding about the scope of Section 5 is unlikely to change at a later stage of the case, Wyndham will have the opportunity to challenge the FTC again at the summary judgment stage, where the FTC will have to produce evidence supporting its claims that Wyndham failed to employ reasonable security and that these failures caused consumers to sustain substantial injuries or at least contradicted representations made to consumers.

It is far from clear that the FTC will be able to make this evidentiary showing. If it cannot, and judgment is granted to Wyndham, then the FTC's ability to pursue companies for data-security failures on unfairness grounds could be almost as badly damaged as it would have been if the court had held that its Section 5 unfairness authority precluded these types of actions. This is because many of the FTC's data-security investigations and settlements have involved breaches of (or other security failures relating to) payment-card information. If incidents involving payment-card data do

not cause substantial, unavoidable injuries, then the FTC may be reluctant to bring these cases—and its targets may be emboldened to challenge the agency as Wyndham has done here.

And even if the FTC prevails in the district court, Wyndham would have the opportunity to appeal to the Court of Appeals for the Third Circuit (and even to the Supreme Court), where it could challenge Judge Salas's rulings on FTC's statutory authority and the need for rulemaking (as well as her conclusions about whether the FTC properly pled and supported its unfairness and deception claims). Wyndham also could seek permission from Judge Salas to immediately appeal these issues.

Given that the case involves novel issues of statutory interpretation, it certainly is possible that other judges may disagree with Judge Salas. If Wyndham were to prevail in the appeals process, it would be a major blow to the FTC's ability to pursue companies for lax data-security procedures. If, on the other hand, the FTC is ultimately successful in this litigation, its victory is unlikely to change the status quo, in which the agency routinely invokes its unfairness authority in taking action against companies for failure to provide reasonable security practices.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our privacy & data security practice group:

Charles Buffon	+1.202.662.5542	cbuffon@cov.com
John Graubert	+1.202.662.5938	jgraubert@cov.com
Kurt Wimmer	+1.202.662.5278	kwimmer@cov.com
Yaron Dori	+1.202.662.5444	ydori@cov.com
David Fagan	+1.202.662.5291	dfagan@cov.com
Stephen Satterfield	+1.202.662.5659	ssatterfield@cov.com