CLIENT UPDATE

COURT GREENLIGHTS FTC'S DATA SECURITY LAWSUIT AGAINST WYNDHAM

NEW YORK
Jeremy Feigelson
jfeigelson@debevoise.com
+1 212 909 6230

Min Lee
mjlee@debevoise.com
+1 212 909 6167

David Sarratt
dsarratt@debevoise.com
+1 212 909 6864

Christopher S. Ford
csford@debevoise.com
+1 212 909 6514

Last week, a federal district judge in New Jersey upheld the Federal Trade Commission's authority to pursue a case charging the Wyndham hotels group with "unfair" and "deceptive" conduct arising out of a series of hacking incidents directed at Wyndham. The court's ruling points the way toward a legal regime where the *victims* of hacking can potentially be held responsible for failing to prevent data breaches if their security measures were deficient.

What happened at Wyndham, what did the court say, and what are the practical takeaways for other companies?

WHAT HAPPENED AT WYNDHAM

According to the FTC's complaint, from 2008 to 2010, hackers were able to steal credit card data and other personal information of about 600,000 Wyndham customers, resulting in more than $10 million in fraudulent charges to their accounts. Notably, the FTC alleged a detailed ticklist of security failures on Wyndham's part:

- failure to employ firewalls to limit access between the public internet, individual hotel servers and the corporate network;
- storage of payment card information in clear readable text;
- permitting insecure servers to connect to Wyndham's networks, using commonly known default user IDs and passwords or outdated operating systems that were incapable of receiving security updates to address known vulnerabilities;
- failure to employ commonly used methods to require user IDs and passwords that were difficult for hackers to guess;
- failure to maintain an adequate inventory of computers with access to Wyndham's servers containing sensitive information;

- failure to monitor its network for malware used in previous intrusions; and
- failure to restrict third-party access to its network, such as by restricting connections to specified IP addresses, or by granting only temporary and limited access.

The FTC charged that Wyndham's alleged failure to take reasonable steps to ensure the security of its customers' data constituted an "unfair" trade practice, while its public assurances regarding its data security practices amounted to "deception." "Unfairness" and "deception" are, of course, the Commission's two main consumer protection standards under Section 5 of the Federal Trade Commission Act of 1914. To oversimplify a bit, the concept of "unfair" conduct covers anything intrinsically harmful to consumers without an offsetting benefit, while "deceptive" conduct is anything contrary to a company's public statements (in this case, a privacy policy that allegedly over-described what Wyndham was actually doing with respect to data security).

WHAT THE COURT SAID

Wyndham brought a wide-ranging threshold challenge to the FTC's case, arguing, among other things, that the FTC lacks any authority to regulate data security and, in the alternative, that any enforcement action must be preceded by clearer Commission statements of the applicable standards of conduct.

Judge Esther Salas of the District of New Jersey ruled for the FTC across the board, denying Wyndham's motion to dismiss. Judge Salas held that the FTC's allegations of security shortfalls by Wyndham, together with the FTC's claim that consumers had suffered actual financial loss resulting from the misuse of their data, were sufficient to state a claim under Section 5 of the FTC Act.

Judge Salas began by upholding the FTC's authority to regulate data security practices that affect consumers, finding no legal basis to carve out a "data-security exception" to the FTC's broad general powers. Further, while recognizing that companies are entitled to some notice of what data-security measures are required, Judge Salas held that the FTC's prior enforcement actions, consent decrees, industry standards and other guidance were sufficient for companies to understand their obligations, noting that standards of "reasonableness" govern in other areas of law as well. Judge Salas was careful to note that her decision "does not give the FTC a blank check to sustain a lawsuit against every business that has been hacked." Rather, the specific allegations against Wyndham, which the FTC alleged did not use industry-standard practices to secure its data and had specifically misled consumers in its privacy policy, meant this case could go forward.

PRACTICAL TAKEAWAYS FOR CORPORATE AMERICA

- *Dog bites man — that is, not much news here, at least as far as the scope of FTC's authority is concerned*. Unfairness and deception are big, flexible legal doctrines that the FTC has been deploying for a century across countless industries and evolving technologies. It is no surprise to see a single district judge being reluctant to embrace Wyndham's aggressive argument for fencing the FTC out of perhaps the hottest area of modern consumer protection law.
- *Don't expect the FTC on your doorstep just because you've been hacked*. Not only did Judge Salas explicitly observe that she was not giving the FTC "a blank check," but as a practical matter the Commission can be expected to devote its limited resources to the biggest and sexiest cases. The Commission has confirmed it is investigating Target, for example. Keep in mind though, that, just as the FTC Act makes "unfair" and "deceptive" conduct illegal, so do equivalent state laws across the country. There are 50 state attorneys general, and innumerable plaintiffs' class-action lawyers, who can be expected to press the case that corporations experiencing future breaches were not just victims, but fell short in an affirmative duty to prevent the breach.
- *Constantly updating your company's data security measures should be seen as a matter of legal obligation*. Chalk up a potentially important win here for the view that the failure to keep data security measures up to snuff is substantively "unfair" and therefore illegal. That view is hardly well-settled in the law, but it gains a bit of a toehold with this decision. So take a look at that list of technical faults pled by the FTC against Wyndham. Internal lawyers should get under the hood and make sure your IT group is doing better than that, and continues to do better as threats evolve.
- *Regularly freshen and tighten your company's online privacy policy and terms of service.* Lofty rhetoric about a commitment to privacy and best security practices can come back to bite you if not honored in the day-to-day.

* * *

Please do not hesitate to contact us with any questions.

April 14, 2014