wiley

NEWSLETTER

FTC Focusing on Service Providers and Stricter Orders in Recent Data Security Case

July 2019

Privacy in Focus®

The Federal Trade Commission's (FTC) recent data security settlement with a company called LightYear Dealer Technologies is notable on a few fronts in what it signals about the agency's direction in data security cases. First, the agency targeted a third party that dealt with consumer data but did not have a direct relationship with consumers, suggesting that it will continue to scrutinize similar kinds of companies. Second, it used a legal theory that potentially signals a more expansive view of the agency's Gramm-Leach-Bliley authority, to reach companies in the tech space. And third, the agency continued to add specific requirements to its data security orders, including by establishing stricter compliance and reporting requirements.

The facts of the case are similar in many ways to those in other FTC data security actions. The agency alleged that the company's software collected sensitive consumer financial, payroll, and other data, that the company did not have certain "reasonable" security measures in place, and that hackers exploited the vulnerabilities to obtain the consumer data. Among other things, the FTC alleged that the company stored personal information in clear text, didn't use "readily available" security measures to monitor attempts to transfer sensitive information, and didn't put certain kinds of access controls in place.

But the case is notable in other ways. First, the defendant did not have a direct relationship with the consumers whose information was hacked. Instead, the company provided software and services to auto dealers to use to manage their own consumer information. The company also enabled the dealers to back up consumer information

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Boyd Garriott
Associate
202.719.4487
bgarriott@wiley.law

Practice Areas

FTC Regulation

Privacy, Cyber & Data Governance

onto the company's network – and that backup network was hacked. Without a direct nexus between the consumer and the defendant, the FTC did not pursue a deception theory, which it often uses in data security cases to argue that a defendant is liable because it made certain representations about securing data to consumers and failed to honor them. Instead, the FTC relied on the theory that the company had committed an "unfair" practice under the FTC Act – a more difficult theory to prove and one that doesn't depend on making representations to consumers. In this case the FTC is making clear that even companies that don't directly deal with consumers can face liability for security breaches.

Second, the FTC asserted another theory of liability that it is not always applicable in data security cases: that the software and service provider is a covered "financial institution" for purposes of the Gramm-Leach-Bliley Act's (GLB) Safeguards Rule, which requires covered entities to take certain steps to safeguard consumer data. While a software provider hardly seems to fit the plain meaning of a "financial institution," the FTC relied on a regulatory provision that sweeps in entities that engage in "data processing" services involving financial, banking, and economic data; the agency pointed specifically to the fact that LightYear's customers were "auto dealerships that extend credit to consumers."

The agency has cited the data processing provision of GLB before, but its application in this case suggests that the FTC could potentially attempt to sweep in many companies – including software companies that provide data-driven services to financial clients – that may not otherwise consider themselves covered financial institutions. The FTC is currently proposing revisions to add requirements to the rule, suggesting that the Safeguards Rule could be a renewed tool for the FTC's enforcement attempts in the data security area.

Finally, the order imposes more specific requirements on this company, a point that the Chairman specifically emphasized in announcing the settlement. Many of these requirements are likely a response to an Eleventh Circuit decision that found one of the Commission's previous data security orders to be too vague. In particular, the order requires annual evaluations of the company's information security program to be provided to the board of directors or governing body and requires a senior corporate manager to provide annual compliance certifications to the FTC. It also requires the company to provide third-party biennial assessments of its information security practices to the Commission. Following the issuance of similar orders in other recent data security cases, this likely points to a shift in FTC data security orders going forward.

As Congress debates whether to increase the FTC's enforcement powers in privacy and data security matters, this latest case shows that the FTC is still using and potentially expanding the tools it already has.