New FTC Data Security Order Shows Trend in Increased Accountability for Data Security Post-Order

JUNE 14, 2019

On June 12, 2019 Lightyear Dealer Technologies LLC, a company that provides data storage for many of the nation's largest auto dealers, stipulated to an Order with the Federal Trade Commission (FTC) resulting from a 2016 data breach that allegedly affected almost 70,000 people. The settlement resulted in a proposed FTC order that imposes standard injunctive provisions on the company, including the development of a comprehensive information security program and submission to bi-annual information security assessments by an independent third-party assessor. The proposed Order will be published in the Federal Register for a 30-day comment period, after which the Commission will consider comments and vote on whether to make the Order final, as is or with modifications.

Orders with such provisions have been issued by the FTC since the Commission began bringing data security cases under Section 5 of the FTC Act's deception and unfairness prongs in the early 2000's, and, with the exception of some company-unique provisions, have remained largely the same since that time. Like other FTC orders, these orders have typically also included boilerplate recordkeeping, reporting, and compliance monitoring provisions.

What's new?

The proposed Lightyear order, however, contains a number of new provisions, reflecting the FTC's effort to update and strengthen its orders, including data security orders under Section 5.[1] Specifically, in addition to an initial and then bi-annual third-party assessments, this proposed order requires that:

(1)The assessor provide specific evidence supporting its conclusion of compliance with the order (this evidence could include independent sampling, employee interviews, or document review);

(2) A senior Lightyear officer personally annually certify the company's compliance with the Order; and

(3) The Commission maintains the authority to approve the assessor for each two-year assessment period.

The FTC was clear in its motives. The press release accompanying the order explained that the "additional and significant improvements" to the orders impose stricter security requirements and are designed to force "company executives to take more responsibility for order compliance." Companies should take note of this, as previous data security orders focused exclusively on the company level, rather than on the individual officer level.

---

* Anna Noone is a Summer Associate in WilmerHale's Washington, DC Office. She is a student at University of Virginia School of Law, class of 2020. Kirk Nahra and Reed Freeman are partners in the Privacy and Cybersecurity Practice Group at WilmerHale in Washington, DC.

[1] This enforcement proceeding also is consistent with the approach suggested by the Federal Trade Commission in a recent Notice of Proposed Rulemaking. On April 4, 2019, the FTC published an NPRM designed to evaluate potential changes to the G-L-B Safeguards Rule. 84 FR 13158 (April 4, 2019). These proposed changes reflect an interest from the FTC in "provid[ing] covered financial institutions with more guidance on how to develop and implement specific aspects of an overall information security program [and] add[ing] provisions designed to improve the accountability of financial institutions' information security programs." This more prescriptive approach may be at odds with the approach of other regulatory agencies, but this current enforcement action indicates that this more precise version of the safeguards Rule may already be in process.