ROPES & GRAY

ALERT

Privacy & Cybersecurity

March 1, 2018

President Trump's FTC Commissioner Nominees Signal Willingness for Greater Data Security Enforcement Authority

Attorneys

Heather Egan Sussman
Douglas H. Meal
James S. DeGraw
Deborah L. Gersh
Seth C. Harrington
Mark P. Szpak
Michelle Visser
David T. Cohen
Kevin J. Angle
Leon Kotlyar

On February 28, 2018, President Trump's four nominees to head the Federal Trade Commission (the "FTC") advanced to the Senate for confirmation and now appear poised to assume leadership of an agency grappling with its data security enforcement powers. Although the FTC has been operating for more than a year under only two commissioners, three short of its full five-seat leadership roster, during that time the agency has nevertheless continued to advance its enforcement authority in this context. At the February 14 confirmation hearing before the Senate Committee on Commerce, Science, and Transportation, all four nominees expressed serious concerns about data breaches, especially the high profile Equifax incident, suggesting that under its new leadership the FTC could embark on even more robust policing of data security practices of American businesses.

Data Breach Concerns Could Result in Expanded FTC Enforcement Authority

At the hearing, the four nominees, led by longtime antitrust attorney Joseph Simons, the nominee for FTC Chair, agreed that responding to data breaches would pose the most important consumer protection challenges for the FTC under its new leadership. Data breaches, according to Mr. Simons, are "becoming much more significant, much more frequent." Christine S. Wilson, who served as chief of staff to Chair Timothy Muris in 2001-02 when they "spent a great deal of time working on data security and consumer privacy issues," predicted that the agency would face a similar workload in the coming years. In accordance with their mutual concern over the severity and frequency of data breaches, all four nominees voiced their commitment to overseeing an agency active on the privacy and data security front.

While the precise contours of the FTC's data security investigation and enforcement priorities under new leadership remain to be developed, expanded authority could come from one of several sources.

First, Mr. Simons and the other nominees welcomed proposed legislation from Senator Richard Blumenthal (D-Conn.) that would grant the FTC authority to impose civil penalties for data security lapses. Mr. Simons stated he was "extremely concerned" about "whether the FTC has sufficient authority to deal with data breaches, particularly in terms of being able to create a sufficient deterrence" and to "create an incentive for companies to take care of the consumer data." Senator Blumenthal's bill, the "Data Breach Accountability and Enforcement Act of 2017" (S. 1900), would enact that very incentive scheme at the federal level by requiring covered entities, including commercial enterprises and all charitable, educational, and non-profit organizations that "acquire, maintain, or use personal information in commerce," to have in place "reasonable cybersecurity protections and practices." The bill would treat a violation of this requirement as an unfair or deceptive act or practice, subject to enforcement and penalty under the FTC Act.

Second, even if Congress does not act, the FTC could continue pushing the envelope of its data security enforcement authority. Last year, the FTC expanded its enforcement in the cloud space by striking a settlement with Uber over the ride-sharing company's alleged misrepresentations regarding its security and employee access practices for personal consumer information. And the FTC continues to litigate over just how "likely" and "substantial" alleged informational injuries must be to trigger the agency's authority to declare a data security practice "unfair" under

Section 5 of the FTC Act. *See LabMD Inc. v. FTC*, No. 16-16270 (11th Cir.) (Ropes & Gray represents LabMD in the appeal). Rohit Chopra, the only Democratic nominee of the group, submitted that data breaches inflict "great deals of cost" upon small enterprises, and in that vein suggested that the FTC consider the "harms that occur to consumers." Mr. Chopra could thus continue championing the FTC's efforts to impose liability for various alleged informational injuries.

New Commissioners Could Oversee More Robust FTC Action

With significant hearing time devoted to data breaches, one incident in particular dominated the colloquy between Senators and nominees. The confirmation hearing suggests that the lessons learned from the Equifax data breach may influence how the new commissioners, once confirmed, address breach responsiveness and notification obligations.

On September 7, 2017, Equifax, one of the three major credit-reporting agencies in the U.S., announced a breach of its security. According to Equifax, it had discovered on July 29 that from May to July intruders had obtained access to the personal information of more than 143 million U.S. consumers, consisting of their names, Social Security numbers, birth dates, and addresses.

In light of Equifax, the nominees responded favorably to questions about enhanced notification requirements. Similar to his solicitude for Senator Blumenthal's proposal, Mr. Simons also expressed interest in a suggestion from Senator Maria Cantwell (D-Wash.) for more rigorous, mandatory notification guidelines. Since an FTC investigation into the Equifax breach is currently ongoing, the nominees were careful to avoid providing specific views as to whether the five-week delay between discovery and public disclosure of the breach was, as Senator Cantwell asked, "too long." But Mr. Chopra nevertheless ventured that, "as a general matter . . . several weeks after a major breach of personal data does not sound like it is fast enough." And Mr. Chopra, recognizing the "patchwork" nature of the largely state-based regulatory landscape governing notification obligations, additionally advocated for the FTC "to be a key partner with attorneys general" on data security matters.

Conclusion

Although the nominees signaled their approval of expanded agency authority and robust action on privacy and data security issues, these inclinations will likely be subject to some internal brakes. For instance, Noah J. Phillips, one of President Trump's nominees and most recently chief counsel to Senator John Cornyn (R-Tex.), acknowledged the importance of data security issues and yet communicated the least preference to building on the agency's data security authority and the most to staying rooted to the agency's core mission. The new commissioners, according to Mr. Phillips, "cannot allow contentious issues to distract us from the bread and butter of the agency on the consumer protection side: looking out for children, veterans, the elderly, and Americans generally."

For more information regarding the nominees to the FTC, or to discuss data security practices generally, please feel free to contact Heather Sussman, Doug Meal, Jim DeGraw, Debbie Gersh, Seth Harrington, Mark Szpak, Michelle Visser, David Cohen, Kevin Angle, Leon Kotlyar, or another member of Ropes & Gray's leading privacy & cybersecurity team.