August 20, 2018

The Honorable Joseph J. Simons
Chairman, Federal Trade Commission
Office of the Secretary
600 Pennsylvania Ave NW
Washington, DC 20580

Subject: Competition and Consumer Protection in the 21st Century Hearings, Project Number P181201

Dear Chairman Simons,

I am writing to offer my perspective on possible changes to competition and consumer protection law, enforcement priorities, and policy in response to your recent solicitation for public comments. As a Member of Congress with a deep interest in protecting US national and economic security interests in cyberspace, I write to suggest areas to improve consumer protection specifically in connection with the Federal Trade Commission's (FTC's) deterrence of unfair and deceptive privacy and data security practices (topic 5, docket FTC-2018-0052).

I applaud the Commission's decision to conduct a broad assessment of its authorities and policies through public hearings. I especially wish to acknowledge the invitation to comment on the efficacy of the Commission's current remedial authority "to deter unfair and deceptive conduct in privacy and data security matters" and offer suggestions for new tools or authorities to increase that efficacy. I am keenly aware that the risks to consumers' data and privacy are continuously expanding and that those risks are all too frequently being realized as incidents.

To date, the Commission's primary enforcement tool to deter unfair or deceptive privacy and data security practices under The Federal Trade Commission Act of 1914, as amended, has been to serve offenders with cease and desist and consent orders. The deterrent efficacy of this approach may be limited, in that the Commission cannot bring a civil action or recover penalties for unfair privacy or data security practices unless a company violates a final order. In effect, companies get a first free pass and must be found to neglect reasonable practices twice before they face a substantial penalty. While a two-strikes approach may be logical for establishing new business practices as unfair or deceptive, I feel the absence of effective privacy or data security programs has been clearly established as injurious to consumers. I am concerned that this remedial approach may provide limited incentive for companies to refrain from unfair practices until after they are caught the first time.

I am further concerned that the Eleventh Circuit Court of Appeals' decision in June in *LabMD vs FTC* may undermine the Commission's use of cease and desist orders to prevent continued unfair and deceptive data security practices. In that decision, the Eleventh Circuit ruled that the Commission's cease and desist order was too vague, as it did not enjoin a specific practice or behavior. In my opinion, this decision does not reflect the dynamic nature of cybersecurity – while reasonable data security outcomes may be fairly static and common from organization to organization, the specific controls to achieve those results are not. Furthermore, it is not the Commission's place to decide what specific controls a company should implement, but rather to evaluate whether those controls are sufficient to avoid constituting an unfair or deceptive practice. Unfortunately, the Court's decision may limit the Commission's ability to issue orders that specify desired outcomes, rather than elaborate on specific controls, to remedy unfair and deceptive data security practices.

In addressing these evolving challenges, I encourage you to work with me and my Congressional colleagues. One potential way to reduce consumer harm is for the Commission to pursue a remedial tool that allows it to impose penalties absent a cease and desist or consent order. Such a tool would incentivize companies to engage in fair business practices without first being investigated by the Commission and would avoid the Eleventh Circuit's concern about court enforcement of vague orders. Another option would be for the Commission to seek authority to establish broadly applicable data security regulations. Such regulations would need to specify desired outcomes and allow for flexibility in implementation, as in the Commission's cease and desist and consent orders to date. Either approach would significantly enhance consumer protections and address shortcomings that currently hamper the Commission's Section 5 enforcement.

Note that, unlike data security, I am not aware of standards or consensus best practices that have emerged for privacy. The ongoing debates about consumers' privacy expectations may warrant continuation of the Commission's issuance of orders in individual cases. I expect that cease and desist orders in privacy matters will not be subject to the same enforceability concerns as for data security.

Separately, the Commission should consider the criteria used to evaluate the Section 5(n) standard of "substantial injury to consumers" in the context of failures to implement reasonable data security or privacy practices. Unlike other unfair and deceptive business practices, negligent handling of consumer information can result in repeated, untraceable injuries that are far removed in time from the practice that caused the injury. Therefore, the burden of proof should reflect the potential for harm. If the Commission can show that sensitive data could be accessed by parties not authorized by the consumer, injury should be presumed. The Commission might clarify this position through orders or, like my earlier suggestions, pursue unique authorities for privacy and data security in regulation or legislation.

I strongly support the FTC's role in enforcing reasonable privacy and data security measures. Failure by a company to protect consumer data is an unfair or deceptive business practice, or both, and liable to cause serious injury to consumers. I encourage the Commission to pursue new tools to better deter negligent data handling, and I appreciate your consideration of my concerns and suggestions.

Sincerely,

CC: Donald S. Clark, Secretary, FTC