United States Senate
WASHINGTON, DC 20510

September 20, 2016

The Honorable Edith Ramirez
Chairwoman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Chairwoman Ramirez:

I write concerning the Federal Trade Commission's (FTC) recent LabMD order and opinion. While I am still reviewing the order and opinion, I have a number of questions about the due process afforded.

LabMD suffered a data breach in 2008. The relevant particulars are that an employee at LabMD used peer to peer (P2P) downloading software that triggered a vulnerability in LabMD's system that allowed a hacker to steal a substantial number of insurance files.

The FTC's administrative law judge (ALJ) dismissed the agency's complaint against LabMD. It did so on the ground that the case lacked any real evidence or likelihood of injury to consumers. The fact that there was a "risk" of such injury, the ALJ concluded, did not satisfy the statute. The agency, in turn, reversed the ALJ and entered an order against LabMD. It concluded that the ALJ had applied an incorrect legal standard and that LabMD's information-security practices were unreasonable and therefore an unfair practice under Section 5 of the FTC Act. It is these facts that I am continuing to review.

However, a more immediate and persistent concern is the extent to which the FTC's cybersecurity regime complies with the protections of due process under the constitution. A recent high-profile cybersecurity case brought by the FTC, *FTC v. Wyndham*, litigated (among other things) the constitutional notice requirement in Section 5 all the way to the Third Circuit. There, the court concluded that the legal standard at play in Section 5 is "a cost-benefit analysis," and that "[f]air notice is satisfied … as long as the company can reasonably foresee that a court could construe its conduct as falling within the meaning of the statute." In other words, whether there is sufficient notice is a question determined as-applied by weighing the costs and benefits of cybersecurity. The court "[a]cknowledge[d] there will be borderline cases where it is unclear if a particular company's conduct falls below the requisite legal threshold [for notice of cybersecurity standards]." As the Third Circuit observed, this legal standard is "far from precise."

With this background in mind, I would like responses to the following questions:

1. The FTC concluded that LabMD's vagueness challenge was distinguishable in part from that in *FCC v. Fox Television Studios, Inc.*, 132 S. Ct. 2307 (2012). This is because "[t]he

regulatory action in *Fox* … directly implicated their First Amendment right to free speech. … No comparable fundamental right is at issue here."

a. Are laws unconstitutionally vague only if they implicate fundamental rights?
b. If not, when may a law that does not implicate fundamental right be found to be unconstitutionally vague?

2. The FTC also concludes in its opinion, "By the same token, 'it is well-established that the common law of negligence does not violate due process simply because the standards of care are uncodified,' and thus 'courts and juries [routinely] subject companies to tort liability for violating uncodified standards of care.'"

a. Should the notice requirements of a regulatory regime codified by statute reflect those of the common law? Why?
b. Is there a constitutional difference between the notice sufficient to sustain a private-law action for negligence and a regulatory one? If so, what?

3. As we noted above, the Third Circuit concluded in the *Wyndham* case that the relevant standard for courts under Section 5(n) is a cost-benefit analysis.

a. What, if any, guidance has the FTC given as to how small businesses are to weigh the costs and benefits of data security?
b. How was the relevant cost-benefit analysis conducted in the Commission's order in LabMD?

4. The FTC concludes in its opinion that agency adjudications "are sufficient to afford fair notice of what was needed to satisfy Section 5(n)." In partial support for this proposition you cite to *United States v. Lachman*, 387 F.3d 42, 57 (1st Cir. 2004). As the First Circuit noted in *Lachman*, however, the statute at issue "deal[t] with economic regulation and is addressed to sophisticated businessmen and corporations which, because of the complexity of the regulatory regime, necessarily consult counsel in planning their activities, and where an administrative process exists to secure advisory interpretations of the statute." *Id.*

a. How does the relative size or sophistication of a business affect the extent to which the FTC's enforcement regime gives it adequate notice of its cybersecurity obligations?

5. The FTC observes in its opinion that "LabMD cannot seriously contend that it lacked notice that its security failures, which led to at least one documented breach of thousands of consumers' sensitive personal information – practices similar to those committed by other companies against which the FTC has taken action – could trigger Section 5 liability." The agency cites two FTC orders predating LabMD's breach as support for this proposition.

a. How many other cybersecurity enforcements had the FTC completed prior to LabMD's 2008 breach?

6. The FTC concludes that "disclosure of sensitive health or medical information" on its own is a "cognizable" injury under Section 5(n).

    a. How, if at all, does the type of sensitive health or medical information disclosed affect the analysis of the injury requirement under Section 5(n)?

We appreciate your attention to this matter and look forward to your response.

Sincerely,

JEFF FLAKE
Chairman
Subcommittee on Privacy, Technology and the Law

MICHAEL S. LEE
Chairman
Subcommittee on Antitrust, Competition and Consumer Rights