Congress of the United States

Washington, D.C. 20515

February 5, 2018

The Honorable Jerry Moran
Chairman
Subcommittee on Consumer Protection,
Product Safety, Insurance, and Data Security
Committee on Commerce, Science, and Transportation
512 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Richard Blumenthal
Ranking Member
Subcommittee on Consumer Protection,
Product Safety, Insurance, and Data Security
Committee on Commerce, Science, and Transportation
716 Hart Senate Office Building
Washington, DC 20510

Dear Chairman Moran and Ranking Member Blumenthal:

We are writing in advance of your hearing titled "Data Security and Bug Bounty Programs: Lessons Learned from the Uber Breach and Security Researchers" to call your attention to Uber's concealment of its 2016 data breach from the Federal Trade Commission (FTC) as it negotiated a consent agreement with the FTC for an earlier breach. We believe that Uber must be held accountable for withholding this information from the FTC. We recently sent a letter to the FTC urging the agency to reopen the consent agreement and reevaluate the adequacy of the remedies imposed on Uber for privacy violations.[1] We have attached a copy of our letter to the FTC for your reference.

Many facts about Uber's year-long cover-up of a breach that affected 57 million customers and drivers are still unknown.[2] We do know, however, that the breach occurred in October 2016, Uber's security team became aware of it in November 2016, and Uber did not notify the FTC until a year later, on November 21, 2017.[3] During that intervening year, as Uber employees were arranging a $100,000 ransom to recover the data and keep the 2016 breach quiet, the FTC was investigating a smaller 2014 data breach and actively negotiating a settlement with Uber regarding that 2014 breach. Uber signed a consent agreement with the FTC on August 15, 2017, without ever informing the agency of the second, much larger breach—one that

[1] Letter from Rep. Jan Schakowsky and Rep. Ben Ray Luján to Maureen Ohlhausen. Acting Chairman, Federal Trade Commission (Dec. 21, 2017).

[2] Letter from Dara Khosrowshahi, CEO, Uber Technologies, Inc., to Sen. John Thune, Chairman, Senate Committee on Commerce, Science, and Transportation, et al. (Dec. 11, 2017).

[3] *Id.*

resulted from a failure to correct the very security vulnerabilities that the FTC investigation of the 2014 breach exposed.[4]

It remains unclear who within the company was aware of the breach for the year preceding disclosure to the FTC. Uber has indicated that two employees were fired for "failing to disclose the incident to the appropriate parties," implying that the breach was not widely known within the company.[5] But it now appears that Uber's former CEO, the legal and communications departments, and as many as 50 engineers may have been involved.[6] Uber's response to the breach was even praised in end-of-year performance reviews of security personnel.[7] It defies credulity that there was not at least some overlap between those aware of the 2016 breach and those responding to the FTC investigation of the 2014 breach. Uber's concealment of critical facts as it negotiated with the FTC is extremely concerning.

Thank you to your Committee for bringing attention to this important issue. We urge you to explore what appears to be serious misconduct by Uber to hide information that would likely have resulted in stronger sanctions in the FTC enforcement action.

Sincerely,

Jan Schakowsky
Ranking Member
House Subcommittee on Digital Commerce
and Consumer Protection

Ben Ray Luján
Member
House Subcommittee on Digital Commerce
and Consumer Protection

Attachment: December 21, 2017 letter to FTC Acting Chairman Maureen Ohlhausen

cc: The Honorable John Thune
The Honorable Bill Nelson

---

[4] Federal Trade Commission, *Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims* (Aug. 15, 2017).

[5] *See* note 2.

[6] *Inside Uber's $100,000 Payment to a Hacker, and the Fallout,* New York Times (Jan. 12, 2016).

[7] Nicole Perlroth (@nicoleperlroth), Twitter (Jan. 12, 2018, 3:38 PM) (twitter.com/nicoleperlroth/status/951961492806541314).

Congress of the United States
Washington, DC 20515

December 21, 2017

Maureen K. Ohlhausen
Acting Chairman
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Dear Acting Chairman Ohlhausen:

I am writing to express my concern regarding recent revelations that Uber Technologies, Inc. was actively concealing a massive data breach at the same time it was negotiating a settlement with the Federal Trade Commission (FTC) for poor privacy and data security practices. In light of this new information, I ask that you consider reopening the public comment period and reevaluate the adequacy of the remedies imposed on Uber in the proposed settlement.

On November 21, 2017, Uber disclosed for the first time that the personal information of 57 million Uber riders and drivers had been stolen by hackers in late 2016.[1] Instead of notifying law enforcement and the public of the breach, Uber paid the hackers a $100,000 ransom in exchange for an agreement to destroy the stolen information and keep the incident secret.[2] Uber took steps to conceal the incident by pushing the hackers to sign nondisclosure agreements and disguising the ransom as legitimate payments from a bug bounty program.[3]

At the same time that Uber was covering up the 2016 breach, the company was negotiating a consent agreement with FTC to address earlier privacy and data security violations.[4] FTC announced the proposed consent on August 15, 2017, before the 2016 breach was made public and presumably without considering the massive scale of the 2016 breach and Uber's cover-up in deciding what remedies were needed to adequately protect consumers.[5] The proposed consent relates to a smaller 2014 breach affecting the personal information of more than 100,000 Uber drivers.[6] FTC's administrative complaint charged Uber only with deceptive practices for making false and misleading statements about its privacy policies.[7] Unlike other recent FTC data security cases, the Uber complaint did not include any charges that the

---

[1] Uber Technologies, Inc., *2016 Data Security Incident* (Nov. 21, 2017) (press release).

[2] *Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data*, New York Times (Nov. 21, 2017).

[3] *Id.*

[4] Federal Trade Commission, *Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims* (Aug. 15, 2017) (press release).

[5] *Id.*

[6] *Id.*

[7] *Id.*

company engaged in unfair practices for failing to adequately protect the information it collected.[8] The proposed administrative consent prohibits Uber from misrepresenting its privacy policies and requires Uber to implement specific steps to enhance its privacy protections and submit to third party auditing.[9] The consent did not include any monetary relief.[10]

Uber's conduct indicates a troubling pattern of disregard for accountability and transparency with respect to its handling of users' personal information. In a statement responding to the proposed agreement, Uber claimed it had "significantly strengthened [its] privacy and data security practices" since 2014.[11] But both the 2014 and 2016 breaches occurred because Uber left employee login credentials exposed in code posted on Github, an online code-sharing repository.[12]

Uber has also repeatedly deceived the public about its privacy practices. The proposed consent agreement addresses Uber's use of a tool known as "God View" to secretly track users without proper notice or oversight.[13] But it does not address the use of another tool known as "Greyball" used to secretly track and evade regulators, which was only disclosed by Uber after a *New York Times* investigation in March 2017.[14]

Dara Khosrowshahi, Uber's new C.E.O. as of August 2017, has since made some changes at Uber in an attempt to distance the company from its previous misconduct, branding it "Uber 2.0."[15] However, larger questions remain about Uber's commitment to meaningfully reforming its leadership and company culture. Only two Uber employees were fired in response to the 2016 breach and subsequent cover-up.[16] Furthermore, Travis Kalanick, Uber's cofounder and C.E.O. until June 2017, still controls a majority of Uber's voting shares and three seats on the company's board of directors.[17] Mr. Kalanick reportedly knew of the 2016 breach and Uber's payments through the bug bounty program since November 2016.[18]

---

[8] *See, e.g.*, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (Aug. 24, 2015) (company's failure to maintain reasonable data security for sensitive personal information resulting in breach fell within the plain meaning of an "unfair" act or practice in violation of Section 5 of FTC act).

[9] *See* note 4.

[10] *See* note 4.

[11] *Uber Agrees to 20 Years of Privacy Audits to Settle FTC Data Mishandling Probe*, TechCrunch (Aug. 15, 2017).

[12] *Uber Hack Shows Vulnerability of Software Code-Sharing Services*, Bloomberg (Nov. 22, 2017); *Uber Paid Hackers to Delete Stolen Data on 57 Million People*, Bloomberg (Nov. 21, 2017).

[13] *Uber Agrees to Privacy Audits in Settlement with F.T.C.*, New York Times (Aug. 15, 2017).

[14] *Uber Settles U.S. Allegations Over Data Privacy*, Reuters (Aug. 15, 2017); *How Uber Deceives the Authorities Worldwide*, New York Times (Mar. 3, 2017).

[15] *Uber 2.0: New C.E.O. Wants to Put His Stamp on the Company*, New York Times (Nov. 9, 2017).

[16] *See* note 2.

[17] *In Power Move at Uber, Travis Kalanick Appoints 2 to Board*, New York Times (Sep. 29, 2017); *Uber Founder Travis Kalanick Resigns as C.E.O.*, New York Times (Jun. 21, 2017),

[18] *Exclusive: Uber Paid 20-Year-Old Florida Man to Keep Data Breach Secret –Sources*, Reuters (Dec. 6, 2017).

Uber's decision to keep the 2016 breach secret for nearly a year raises serious concerns about whether Uber was negotiating with FTC in good faith, and about whether the company has the intention and ability to properly administer the proposed consent. I therefore request a briefing on this matter with my staff and Committee staff. Please be prepared to discuss the following questions.

1. When did Uber first inform FTC of the 2016 breach and Uber's response? Was FTC aware of the 2016 breach and Uber's response when the Commission approved the proposed consent in August 2017?

2. It is our understanding that at least 20 Uber employees, as well as the C.E.O., were aware of the 2016 breach at the time Uber was negotiating with FTC. Given this, was the termination of only two employees in response to the 2016 breach sufficient to ensure the culture has changed and that Uber is likely to comply with the proposed consent?

3. Did Uber fail to comply with the terms of any civil investigative demand by withholding documents, information, or other relevant evidence related to FTC's investigation, including any evidence related to the 2016 breach and the company's response?

4. Did Uber violate any laws or regulations, including provisions related to preservation of records or making false statements, by destroying any evidence, by failing to disclose the 2016 breach and its response to that breach in the course of FTC's investigation, or any other action?

5. Is FTC conducting a separate investigation of Uber's "Greyball" tool? Did the Commission consider Uber's use of the "Greyball" tool when voting to approve the proposed consent?

6. Given that the 2014 breach involved personal information from over 100,000 Uber drivers including, for a subset of those drivers, Social Security number and bank account numbers, why did FTC not challenge the breach as both deceptive and unfair?

7. Has the Commission considered whether consumers would be better served if the Commission reopened its case against Uber and issued a new complaint in federal court, under Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), that would include new charges on the 2016 breach and cover-up and seek broader remedies, including monetary relief?

Your assistance in this matter is greatly appreciated.

Sincerely,

Ben Ray Luján
Member
Subcommittee on Digital Commerce
and Consumer Protection

Jan Schakowsky
Ranking Member
Subcommittee on Digital Commerce
and Consumer Protection