United States Senate
WASHINGTON, DC 20510-0905

December 1, 2017

Mr. Dara Khosrowshahi
Chief Executive Officer
Uber Technologies, Inc.
1455 Market St.
San Francisco, CA 94102

Dear Mr. Khosrowshahi:

We write today to request information on a 2016 data breach that affected Uber customer and driver accounts. Media reports indicate that data on approximately 57 million Uber users was compromised in this breach, including names, phone numbers, and email addresses. In addition, Uber driver information was also accessed, including driver's license numbers. This breach shows a pattern and practice of Uber not properly securing data or notifying those affected by such a breach, similar to the data breach that Uber suffered in 2014.

In 2014, Uber data was breached in May and discovered in September, but not made public until February 2015. After the 2014 breach, Uber settled with the Federal Trade Commission (FTC) after the agency found that Uber did not implement basic security practices such as encryption or two-factor authentication to keep its data safe. The consent order prohibits Uber from misreprenting its privacy and data security practices. Uber also agreed to submit its privacy practices to regular audits by an outside firm the next 20 years. The fact that Uber has suffered a massive data breach soon after the FTC investigation and settlement calls into question Uber's corporate commitment to data privacy and security.

Notwithstanding the fact that this breach occurred over a year ago, Uber only recently made the breach known to the public after paying the hackers a ransom of $100,000 to delete the stolen information. This breach, the long delay in reporting it, and an apparent attempt to cover it up by paying a ransom illustrate problems that we raised back in December 2014 when we sent a letter noting troubling problems with Uber's data security and privacy policies and requesting information on Uber's handling of sensitive consumer information.

Specifically, on December 19, 2014, we sent a letter to Uber's then Chief Executive Officer, Travis Kalanick, requesting detailed information on the company's privacy and data security policies. In particular, we asked for all relevant documents, both public and private, pertaining to Uber's practices regarding the collection, use, and sharing of customer information, including how that data is secured from an unauthorized breach. We received a response in the form of a letter dated January 9, 2015, from Ms. Katherine M. Tassi, the Managing Counsel for Privacy, which did not provide the documentation as requested.

The questions we raised in our December 2014 letter are still relevant today with regard to Uber's data breach. In particular, we asked that Mr. Kalanick provide us with copies of practices pertaining to "data security measures Uber has in place to protect its customers' data from a potential breach." In response, Ms. Tassi wrote that "Uber has in place standard measures to protect the security of its network and rider personal data" and that it further "has written incident response procedures in the event that our network is breached." However, Uber failed to provide us with the requested documentation of these practices.

Furthermore, in addition to being unresponsive, it appears that some of the responses may have been materially misleading. According to media reports, a former Uber employee testified in a November 28, 2017, hearing in litigation between Uber and Waymo that Uber operated a clandestine unit dedicated to stealing trade secrets and used secret servers and communicated through self-destructing messaging platforms. To the extent that this alleged unit handled any consumer or driver information, it may have provided a entry path for hackers. Furthermore, the omission of its existence, process for handling information, or data privacy practices from any customer notice may, at best, be a false and deceptive trade practice.

As the Ranking Members of the Senate Committee on Commerce, Science, and Transportation and the Committee on Homeland Security and Governmental Affairs, we have long advocated for strong data security legislation to protect American consumers from the unauthorized access and use of their sensitive information. As such, we ask that Uber provide the following information, some of which was part of our original 2014 request:

1) The date the 2016 breach occurred and how and when it was detected.

2) The total number of current and former Uber customers, drivers, and employees whose data was compromised by the breach, as well as a description of the type of information that was accessed in the breach. Include a complete accounting of all types of data compromised, including, but not limited to, geolocation data, physical addresses, personally identifiable information, financial information, etc.
3) Whether notification of the breach has been provided to impacted Uber customers, drivers, and employees. If not, whether Uber anticipates providing such notification in the near future and how it will provide that notification.
4) Whether Uber intends to offer identity theft or credit monitoring protection to customers, drivers, and employees impacted by the breach. If so, indicate whether such monitoring will be offered for free and the duration of the services.
5) A list of all regulators Uber has notified about the breach, how they were notified, and on what dates these notifications occurred.
6) The date that Uber first made contact with the party or parties that accessed customer and driver information.
7) The date that Uber made any "ransom" payments to the party or parties who accessed customer and driver information, the name of the party or parties to whom the payments were made, and the method by which funds were transferred to the party or parties.
8) Whether a non-disclosure agreement or any similar legal document was executed between Uber and the party or parties to which "ransom" payments were made. If any such agreements were executed, please provide copies of the agreements.
9) Whether Uber, at any point, operated a clandestine unit that dealt with trade secret information. If so, please detail the operations of this unit, whether it handled any consumer or driver information, the privacy practices of this unit, and whether it was involved in the 2016 breach.
10) Whether an outside cybersecurity firm has been retained to examine the circumstances of the breach. If so, please identify the firm and describe the scope of the work. Also, identify if analysis, investigation, review, or forensics done by an outside company, Uber, or any law enforcement agency has indicated that any additional information was stolen or compromised.
11) Any and all of Uber's privacy policies since the company's inception, including when and how those polices have changed over time.
12) The audit reports of Uber's privacy practices from the outside company required by the FTC to be used after the 2014 data breach.
13) Uber's specific policies regarding the sharing or selling of customer data, including when and how those policies have changed over time.

14) The extent to which Uber retains data on current and former Uber customers, drivers, and employees, including the type of data retained, the period of time such data is retained, who in the company has access to such data, how the data is secured, and when and how Uber's practices regarding data retention have changed over time.
15) Uber's practices regarding notifying customers about its privacy and data security policies related to customer data, and any changes to those policies from November 18, 2014, to the present.
16) The data security measures Uber had in place to protect the data of its customers, drivers, and employees from a potential breach on November 18, 2014, when the 2016 breach occurred, as well as Uber's current policies.
17) The data security measures Uber put in place as a result of the 2014 data breach and the FTC investigation in 2015.

Thank you for your prompt attention to this request. We look forward to hearing from you as soon as possible but no later than December 14, 2017.

Sincerely,

Bill Nelson
United States Senator

Claire McCaskill
United States Senator