

United States Senate

WASHINGTON, DC 20510

November 27, 2017

Mr. Dara Khosrowshahi
Chief Executive Officer
Uber Technologies, Inc.
1455 Market Street
San Francisco, CA 94103

Dear Mr. Khosrowshahi:

We write today regarding reports that, in late 2016, Uber learned that it had suffered a significant data security incident. Hackers apparently accessed user data including the names and driver's license numbers of about 600,000 drivers in the United States as well as the personal information of 57 million Uber users around the world, including names, e-mail addresses, and mobile phone numbers.¹

Perhaps more troubling, several media reports indicate that, rather than report the incident to regulators or to affected customers, Uber instead paid \$100,000 to the hackers to delete the stolen data, allegedly to conceal the breach.²

The company maintains that its outside forensic experts have not seen any indication that customer trip location history, credit card numbers, bank account numbers, Social Security numbers, or dates of birth were downloaded.³ Nevertheless, the nature of the information currently acknowledged to have been compromised, together with the allegation that the company concealed the breach without notifying affected drivers and consumers, and prior privacy concerns at Uber, makes this a serious incident that merits further scrutiny.

In January 2015, Uber released a report entitled "Review and Assessment of Uber's Privacy Program."⁴ The review that Uber's outside counsel conducted determined that Uber had in place "appropriate policies and procedures" in several areas, including data security, incident management and response, data retention, and accountability.⁵ Though a technical audit was not part of this review, the report found that, "Uber has put in place and continues to develop a data security program that is reasonably designed to protect Consumer Data from unauthorized

¹ Dara Khosrowshahi, *2016 Data Security Incident*, UBER NEWSROOM (Nov. 21, 2017), <http://www.uber.com/newsroom/2016-data-incident>.

² See, e.g., Eric Newcomer, *Uber Paid Hackers to Delete Stolen Data on 57 Million People*, BLOOMBERG TECH., Nov. 21, 2017, <http://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data>.

³ Khosrowshahi, *supra* note 1.

⁴ Hogan Lovells, *Review and Assessment of Uber's Privacy Program* (Jan. 2015), <https://newsroom.uber.com/wp-content/uploads/2015/01/Full-Report-Review-and-Assessment-of-Ubers-Privacy-Program-01.30.15.pdf>.

⁵ *Id.* at 1.

access, use, disclosure, or loss.”⁶ It further details administrative, technical, and physical safeguards for data protection, as well as company policies for reporting and responding to data breaches.⁷ Despite the safeguards in place, according to recent reports, Uber’s board commissioned an investigation by an outside law firm, which discovered the recently revealed hack and the failure to disclose it.⁸

Additionally, the Federal Trade Commission (FTC) announced on August 15, 2017, that Uber agreed to a consent order addressing its privacy and data security practices. Among other things, the order prohibits Uber from misrepresenting the extent to which it protects the privacy, confidentiality, security, or integrity of any personal information.⁹ The order also requires Uber to implement a comprehensive program to protect the privacy and confidentiality of the personal information it collects and maintains.¹⁰

Our goal is to understand what steps Uber has taken to investigate what occurred, restore and maintain the integrity of its systems, and identify and mitigate potential consumer harm and identity theft-related fraud against Federal programs. Accordingly, we request answers to the following questions:

1. On what date did Uber first learn that hackers accessed user data stored on a third-party cloud-based service?
2. How many consumers does the incident affect, including riders and drivers? Please describe Uber’s efforts to identify and provide notice to the affected individuals.
3. With respect to the incident, what types of data does Uber believe to have been compromised? To what extent does the data include sensitive personal information?
4. Did Uber authorize payments to outside parties in connection with the incident? If so, please provide additional details, including the amounts, dates, method of transfer, as well as the purpose of such payments, including whether the purpose of such payments was, even in part, to conceal the incident itself. Who authorized these payments?
5. Which regulators has Uber notified about the incident? On what dates did these notifications occur?
6. Beyond monitoring affected accounts, what steps has Uber taken to identify and mitigate potential consumer harm associated with this incident?
7. What steps has Uber taken to ensure compliance with its obligations under the FTC order, such as its obligation to establish, implement, and maintain a comprehensive privacy program?

⁶ *Id.* at 2.

⁷ *Id.* at 22-25.

⁸ Newcomer, *supra* note 2.

⁹ Press Release, Fed. Trade Comm’n, Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims (Aug. 15, 2017), <https://www.ftc.gov/news-events/press-releases/2017/08/uber-settles-ftc-allegations-it-made-deceptive-privacy-data>.

¹⁰ *Id.*

Mr. Dara Khosrowshahi

November 27, 2017

Page 3

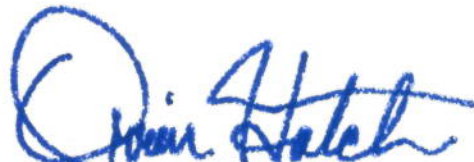
8. Did Uber disclose the incident to the FTC during the agency's investigation that led to the consent order? If so, when? If not, why not?
9. What personnel actions has Uber taken in response to the incident? Please provide specific details.
10. Please provide a detailed timeline of events, including Uber's initial discovery of the incident, forensic investigation and subsequent security efforts, notifications to law enforcement agencies and regulators, as well as any notification to affected consumers.
11. Uber has maintained that the hackers did not download social security numbers. Did the breach involve the compromise of social security numbers in any way? Please provide a complete description, including any related forensic analysis.

We look forward to receiving your responses as soon as possible, but by no later than 5:00 p.m. on December 11, 2017. In addition, please direct your staff to make arrangements to brief our staffs on this matter by no later than December 1, 2017. Thank you for your prompt attention to this matter.

Sincerely,



JOHN THUNE
Chairman
Committee on Commerce,
Science, and Transportation



ORRIN HATCH
Chairman
Committee on Finance



JERRY MORAN
Chairman
Subcommittee on Consumer
Protection, Product Safety,
Insurance, and Data Security



BILL CASSIDY, M.D.
Chairman
Subcommittee on Social Security,
Pensions, and Family Policy

cc: The Honorable Bill Nelson, Ranking Member
Committee on Commerce, Science, and Transportation

The Honorable Ron Wyden, Ranking Member
Committee on Finance

The Honorable Richard Blumenthal, Ranking Member
Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security

The Honorable Sherrod Brown, Ranking Member
Subcommittee on Social Security, Pensions, and Family Policy