

# United States Senate

WASHINGTON, DC 20510

September 16, 2015

Sergio Marchionne  
Chief Executive Officer  
Fiat Chrysler  
1000 Chrysler Dr.  
Auburn Hills, MI 48321

Dear Mr. Marchionne,

We write to request information regarding your company's efforts to protect the privacy and security of the cars it sells. As vehicles become increasingly connected to the Internet and to one another through advanced features and services, we continue to see how these technologies present vulnerabilities that can compromise the safety and privacy of drivers and passengers. We have specifically learned how third parties can access the electronic controls and data of vehicles from many different entry points, including wireless connections, and we appreciate that many automotive companies have begun to take concrete steps to close these security gaps.

In the attached letter dated December 2, 2013, your company was asked to provide information about the technologies and capabilities of new vehicles as well as efforts to protect consumer privacy and security. Your response proved invaluable in understanding these practices.

We write now to request an update to the information you provided regarding your company's protections against the threat of cyber-attacks or unwarranted invasions of privacy related to the integration of electronic systems into and within automobiles.

Today's cars and light trucks contain increasing numbers of electronic control units, connected through a control area network (CAN) or other central system. Vehicle functionality, safety, and privacy all depend on the functions of these computers, as well as their ability to communicate with one another. They also have the ability to record vehicle data to analyze and improve performance. However, a series of studies over the past few years have demonstrated how these systems can be remotely hacked to steal data or take control of the vehicle away from the driver. A recent high-profile hacking demonstration was performed wirelessly from miles away while the vehicle was on a highway, showing how hackers could control the air conditioning, windshield wipers and fluid, radio, transmission, and later while the vehicle was in a parking lot, the brakes and steering.<sup>1</sup> Even more recently, security experts were able to hack into an OBD2 dongle (a web-connected device used to provide third parties with information about vehicles' speed, location and other characteristics) by sending carefully-crafted text messages, showing that they were able to activate the windshield wipers and disable the vehicle's brakes.<sup>2</sup>

---

<sup>1</sup> <http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>

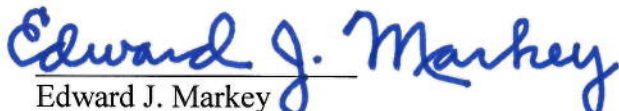
<sup>2</sup> <http://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/>

Based on the responses from the initial letter, Senator Markey released the February 2015 report *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk*<sup>3</sup>. This report details how while nearly every new vehicle on the road includes some type of wireless technology, very little has been done to secure vehicles against hackers trying to steal information or take control of a vehicle. Additionally, the ways that manufacturers are handling sensitive driving data and making consumers aware of data collection and use was alarming. In response, the Alliance of Automobile Manufacturers and the Association of Global Automakers released a set of voluntary privacy standards to ensure that consumer data is secure. While we are pleased that the industry has taken a step in the right direction, we believe that protecting the safety, security and privacy of American drivers should not be voluntary. Consumers should have meaningful choice and transparency regarding any collection of their data derived from driving their vehicles. The voluntary industry measures also fail to adequately address rising cybersecurity concerns.

We ask that you please respond to the 2013 letter, providing updated information as appropriate and providing company-specific information that includes your MY 2015 and 2016 vehicles. Please additionally provide a description of any changes to your company's vehicle fleet or characteristics, policies, practices and experiences that may have occurred since your company first responded to Senator Markey's original letter.

Thank you for your attention to this important matter. Please provide your response no later than Friday October 16, 2015. If you have any questions, please have a member of your staff contact Michal Freedhoff or Joseph Wender at 202-224-2742.

Sincerely,

  
Edward J. Markey  
United States Senator

  
Richard Blumenthal  
United States Senator

[Attachment: 12/2/2013 letter]

---

<sup>3</sup> [http://www.markey.senate.gov/imo/media/doc/2015-02-06\\_MarkeyReport-Tracking\\_Hacking\\_CarSecurity%202.pdf](http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf)