United States Senate
WASHINGTON, DC 20510

August 22, 2019

Deputy Administrator Heidi King
National Highway Traffic Safety Administration
1200 New Jersey Avenue, SE
Washington, DC 20590

Dear Deputy Administrator King:

We write to ask whether the National Highway Traffic Safety Administration (NHTSA) has received information from automakers regarding the cybersecurity vulnerabilities of their internet-connected cars. According to a recent report, companies such as BMW, Daimler Chrysler, Ford, General Motors, and Tesla have acknowledged the dangers of internet-connected cars to their investors and shareholders, but have not disclosed these same risks to the public at large.[1] We are concerned that consumers are purchasing internet-connected vehicles without sufficient safety warnings and write to inquire about NHTSA's knowledge of any cyber vulnerabilities, as well as what actions NHTSA is taking to address these issues.

Today, there are approximately 50 million cars on U.S. roads with safety-critical systems that are connected to the internet.[2] By 2022, two-thirds of all new cars will include internet-connected features and systems.[3] The proliferation of increasingly computerized cars raises significant cybersecurity and public safety risks. Most alarmingly, connected vehicles can potentially be hacked and remotely controlled by malicious actors, creating risks not only to the lives of car drivers and passengers, but also to pedestrians and property along the road.[4]

According to their own investor filings, automakers are aware of these dangers. For example, in a 2018 filing with the Securities and Exchange Commission, Ford described how its "[o]perational systems, security systems, and vehicles could be affected by cyber incidents."[5] Ford specifically reported that:

> Despite security measures, we are at risk for interruptions, outages, and breaches of: (i) operational systems . . . (ii) facility security systems; and/or (iii) in-vehicle systems or mobile devices. Such cyber incidents could materially disrupt operational systems . . . compromise the privacy of personal information of customers, employees, or others . . . affect the performance of in-vehicle systems; and/or impact the safety of our vehicles. A cyber incident could be caused by malicious third parties using sophisticated, targeted methods to circumvent

---

[1] CONSUMER WATCHDOG, KILL SWITCH: HOW CONNECTED CARS CAN BE KILLING MACHINES AND HOW TO TURN THEM OFF 12-15 (2019), https://www.consumerwatchdog.org/sites/default/files/2019-07/KILL%20SWITCH%20%207-29-19.pdf.
[2] *Id.* at 6.
[3] *Id.* at 2.
[4] *Id.* at 2, 43.
[5] Ford Motor Company, 2018 Annual Report (Form 10-K) Page 18 (Feb. 21, 2019), https://s22.q4cdn.com/857684434/files/doc_financials/2019/annual/ford-10k.pdf.

> firewalls, encryption, and other security defenses, including hacking, fraud, trickery, or other forms of deception. We, our suppliers, and our dealers have been the target of these types of attacks in the past and such attacks are likely to occur in the future.[6]

Yet, despite this awareness and their notice to investors, Ford and other automakers have marketed internet-connected cars to the public without disclosing these potential cyber vulnerabilities.

We are concerned by the lack of publicly available information about the occurrence and handling of cyber vulnerabilities in internet-connected cars, and believe that NHTSA should be aware of these dangers in order to take possible regulatory action. We therefore ask that NHTSA answer the following questions:

1) Has NHTSA ever been notified of malicious hacking attempts against or vulnerabilities in internet-connected cars, such as those identified in Ford's statements to investors?
    a. If NHTSA was notified of any such attempts, what actions did NHTSA take in response to the information? If no action was taken, why not?
    b. Further, if NHTSA was notified, why was the public not informed of the cyber risks to any vehicles they already owned or were considering purchasing?

2) What actions has NHTSA taken, and what actions does NHTSA plan to take, in order to address the cyber vulnerabilities and public safety risks created by the increasing number of internet-connected cars on U.S. roads?

3) Does NHTSA have a formal process in place to receive reports of hacking or vulnerabilities in internet-connected cars?

4) In the event of a cyber incident or vulnerability involving the security of an internet-connected car, what entity would be expected to provide public disclosure? Would that public disclosure be legally required?

Thank you for your attention to this important matter. We respectfully request that you provide a written response to these questions by September 13, 2019.

Sincerely,

Edward J. Markey
United States Senator

Richard Blumenthal
United States Senator

---

[6] *Id.*