Counsel's Advisory
Vol. 28 No. 1 April 24, 2020

Washington Legal Foundation
Advocate for Freedom and Justice®
2009 Massachusetts Avenue, NW
Washington, DC 20036
202.588.0302 wlf.org

Federal Court Stalls Plaintiff Class Actions in Jeep Hacking Case for Lack of Standing

by Gregory A. Brower and Samantha J. Reviglio

On March 27, 2020, a federal district judge in Illinois dismissed a certified class action aimed at alleged defects in the Jeep Cherokee Uconnect system that exposed the vehicle to computer hackers.[1] U.S. District Judge Staci M. Yandle found "conclusory and unsupported" plaintiffs' allegations that the defendants wrongfully induced them to purchase their vehicles by concealing a defect in the vehicles' onboard computer system. This marks a significant defeat for three different classes of more than 220,000 plaintiffs.

Plaintiffs first alleged in 2015 that certain Fiat Chrysler ("FCA") vehicles were "dangerously vulnerable to cyberattacks" that would grant hackers access to the vehicles' steering, braking, acceleration, and ignition. From the outset, defense attorneys argued that the plaintiffs lacked standing because they had not suffered actual, concrete injuries. Indeed, none of the plaintiffs' vehicles had ever been hacked. The only known hack was contrived in an experiment two online researchers conducted for a 2015 *Wired* magazine article. The article detailed how the skilled researchers remotely accessed a Jeep Cherokee's UConnect infotainment system and took control of the vehicle while it was being operated on a highway. Fiat Chrysler immediately issued a voluntary recall of about 1.4 million vehicles equipped with this system and later announced that it had corrected the system flaw to the satisfaction of the National Highway Traffic Safety Administration. Nevertheless, the plaintiffs' lawyers still sued.

Judge Yandle's decision slammed the brakes on the five-year old litigation. In her ruling, Judge Yandle relied upon a Ninth Circuit decision, *Cahen v. Toyota*,[2] in which the court held that an alleged future risk of hacking and the economic losses tied to that hypothetical harm are much too speculative to support standing. She observed that "[a]s was true in *Cahen*, there has been no demonstrable effect on the market for plaintiffs' vehicles based on, for example, documented recalls, declining Kelley Bluebook values, or a risk so immediate that they were forced to replace or discontinue using their vehicles, thus incurring out-of-pocket damages."[3] "Ultimately, plaintiffs have not suffered any injury in fact," the judge concluded.

This decision is not only a victory for Fiat Chrysler, but also for many other "Internet of Things" product manufacturers that face exposure to lawsuits based solely on fear of malicious hacking. With so many products—refrigerators, baby monitors, thermostats, etc.—theoretically vulnerable to hacking, claims like those made in *Flynn* could adversely impact the development of innovative products that improve consumers' lives in untold ways. *Flynn* clarifies that claims of purely hypothetical cybersecurity vulnerabilities cannot and should not proceed to trial.

---

[1] *Flynn et al., v. FCA, US LLC and Harman International Industries, Inc.*, Case No. 15-cv-855-SMY, 2020 WL 1492687 (S.D. Ill. Mar. 27, 2020).
[2] 717 Fed. Appx. 720 (9th Cir. 2017).
[3] *Flynn*, 2020 WL 1492687 at * 5.

Gregory A. Brower is a Shareholder with Brownstein Hyatt Farber Schreck, LLP in Las Vegas, NV and Washington, DC and **Samantha J. Reviglio** is an Associate with the firm in its Reno, NV office. Mr. Brower is a member of WLF's Legal Policy Advisory Board.

 ISBN 1056 3059