Counsel's Advisory
Vol. 27 No. 2 February 15, 2019

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

Case Involving Automobile's Hacking Vulnerability Allowed to Proceed to Trial

by Gregory A. Brower and Samantha J. Reviglio

In 2015, Fiat Chrysler announced the automobile industry's first ever recall related to a cybersecurity "defect." The recall affected 1.4 million vehicles equipped with the uConnect infotainment system following the publication of an internet article by a group of online researchers claiming to have found vulnerabilities in the system. Fiat Chrysler stated that any defect in the infotainment system was corrected to the satisfaction of the National Highway Traffic Safety Administration ("NHTSA"). However, a class-action lawsuit was soon filed in the Southern District of Illinois, *Flynn, et al. v. FCA US, et al.*, and it may be one of the first cases involving the potential hackability of automobiles to proceed to trial.

In *Flynn*, plaintiffs allege that certain Jeep Grand Cherokee models posed a risk of injury or death because its infotainment systems were vulnerable to hacking. Hackability claims were previously made in a similar class-action filed in 2015 in the Northern District of California, *Cahen, et al. v. Toyota Motor Corp, et al.*, involving Toyota, Ford, and General Motors vehicles. The District Court dismissed the case, 147 F. Supp. 3d 955 (N.D. Cal. 2015), and the U.S. Court of Appeals for the Ninth Circuit affirmed the decision, unanimously concluding that the plaintiffs failed to allege a "concrete and particularized" injury. 717 Fed. Appx. 720 (9th Cir. 2017).

The claims in *Flynn* follow an experiment conducted by researchers who ultimately published an article describing how hackers were able to remotely access the vehicle's system while a Jeep was traveling on a highway. Most observers assumed the Southern District of Illinois would reject hackability claims in the *Flynn* case, which also involved no injuries, for the same reasons the plaintiffs' claims in the *Cahen* case were rejected. While the district court did dismiss the theoretical claims alleging damages of injury or death, it surprisingly allowed the plaintiffs' claims for damages based on a theory of diminution in value to proceed. 2016 WL 5341749 (S.D. Ill., Sept. 23, 2016).

FCA appealed to the Seventh Circuit, alleging under Federal Rule of Civil Procedure 23(f) that the district court committed a "manifest error" in finding that Flynn had standing to sue. The Seventh Circuit rejected the appeal. No. 18-8010 (7th Cir., May 4, 2018). FCA petitioned for writ of certiorari to the U.S. Supreme Court. On January 7, 2019, the Court denied cert, setting the stage for a trial on the merits in the Southern District of Illinois.

Cases that target "smart" or "internet of things" ("IoT") devices alleging nothing more than an alleged potential vulnerability to hacking present a novel new theory of liability for manufacturers and sellers of a wide range of products. Today, even the most common household items such as refrigerators, light bulbs, baby monitors, and thermostats are, to some extent, IoT devices, theoretically vulnerable to hacking. To allow such claims to proceed past the summary judgment stage, based upon nothing more than allegations of theoretical harm with no actual damages, could potentially undermine the development and marketing of the innovative products customers want, thus harming the very consumers our tort system is supposed to protect.

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