THOMSON REUTERS
Westlaw®

Jeep drivers' claims come to a screeching halt: Hypothetical hacking threat does not confer Article III standing

By Melissa DiGrande, Esq., *Proskauer Rose LLP**

MAY 5, 2020

On March 27, 2020, a five-year legal battle between three certified classes of Jeep Cherokee drivers and Fiat Chrysler came to a sudden end, when a federal judge in the Southern District of Illinois held[1] that allegations that the vehicles were vulnerable to cyber-attacks did not give plaintiffs standing to sue under Article III of the Constitution.

U.S. District Judge Staci M. Yandle — who was assigned to the case in April 2019, after Judge Michael Reagan retired — did not take lightly her decision to grant defendants' motion to dismiss for lack of jurisdiction, given the lengthy history of the dispute.

Discovery had been completed, experts had been retained, and several motions involving the same standing issues had already been resolved — in plaintiffs' favor.

But, as Judge Yandle explained, a federal court has "an independent obligation at each stage of the proceedings" to ensure that it has subject matter jurisdiction over the litigation. Ultimately, defendants' persistence paid off and resulted in the full dismissal of the claims, with prejudice.

The allegations in *Flynn et al. v. FCA US LLC et al.* centered on the "Uconnect" infotainment system installed in some of FCA's 2013-2015 model vehicles.

The Uconnect system provides drivers with integrated control over the vehicles' phone, navigation, and entertainment functions. The system was manufactured by Harman International Industries, Inc., another named defendant.

According to the *Flynn* plaintiffs, the Uconnect system is defective because of its vulnerability to cyber-attacks: hackers can theoretically take control of the vehicle remotely by accessing the vehicles' critical safety systems, including steering, braking, acceleration, and ignition.

Plaintiffs' expert also suggested that a lack of additional safety features — such as secure gateways, trust anchors, and intrusion detection — rendered the system "unreasonably dangerous" and defective.

In building their case against FCA and Harman, plaintiffs relied heavily on a 2015 article featured in *WIRED* magazine[2], which described an elaborate, controlled experiment in which highly trained researchers were able to remotely access the Uconnect system in the test vehicle, a Jeep Cherokee.

Notably, none of the plaintiffs alleged that their own vehicles had been hacked or that they had otherwise stopped driving the vehicles on account of the alleged defect.

> As plaintiffs conceded, the experiment described in *WIRED* was the *only* instance — out of 1.2 million vehicles — involving an actual cyber-attack on the vehicles in question.

Nonetheless, plaintiffs insisted they suffered economic harm as a result of these "defects," because they would not have purchased (or would have paid less for) the vehicles but for defendants' misrepresentations about the system's alleged defects.

They also argued that the defects have diminished the resale value of the vehicles.

Judge Yandle summarily rejected these theories in a 10-page memorandum and order.

Standing under Article III requires:

(1) an injury in fact

(2) that is fairly traceable to the challenged conduct of the defendant and

(3) likely to be redressed by a favorable judicial decision.

Here, Judge Yandle's decision granting the motion to dismiss focused largely on the first prong: plaintiffs' failure to allege concrete, actual harm.

As an initial matter, Judge Yandle questioned whether plaintiffs had sufficiently alleged that the Uconnect system was defective at all.

As plaintiffs conceded, the experiment described in *WIRED* was the *only* instance — out of 1.2 million vehicles — involving an actual cyber-attack on the vehicles in question.

By contrast, the cases relied upon by plaintiffs all involved demonstrably defective products that had actually malfunctioned and/or were clearly unusable due to the defects.

Judge Yandle emphasized that no product is completely foolproof, and "[t]he fact that the Uconnect has vulnerabilities and could have been made safer does not make it defective when no vehicles have ever manifested the alleged defect."

Judge Yandle similarly found plaintiffs' allegations of economic harm to be too speculative to satisfy the injury-in-fact requirements of Article III.

On this point, Judge Yandle relied in large part on *Cahen v. Toyota Motor Corp.*, 147 F. Supp. 3d 955,[3] *aff'd, Cahen v. Toyota Motor Corp., 717 Fed. App'x 720,*[4] a case involving nearly identical claims that the defendants equipped their vehicles with technology that was highly vulnerable to third-party hacking.

The Northern District of California determined that the plaintiffs failed to plead facts sufficient to establish Article III standing, and the Ninth Circuit affirmed.

Although the Ninth Circuit's decision is unpublished, Judge Yandle found the reasoning of the case to be particularly compelling, given the factual similarities to the *Flynn* case.

In particular, the plaintiffs in both *Cahen* and *Flynn* failed to allege a demonstrable effect on the market to support their "overpayment" theory.

For instance, neither set of plaintiffs pointed to "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."

Judge Yandle emphasized that the *Flynn* plaintiffs had not alleged that they were unwilling to drive the vehicles as a result of the defects, nor had any of the plaintiffs sold or traded (or attempted to sell or trade) their vehicles at a loss as a result of the defects.

Ultimately, Judge Yandle held that any claims that plaintiffs were "induced" by defendants to purchase these vehicles by "concealing" the alleged defect, or that the vehicles are worth substantially less than they would be without the alleged defect, are conclusory and unsupported.

Judge Yandle similarly found plaintiffs' allegations of economic harm to be too speculative to satisfy the injury-in-fact requirements of Article III.

To the contrary, she found that the plaintiffs received precisely "what they bargained for — vehicles equipped with infotainment services."

Judge Yandle's decision is a significant victory for FCA, which no longer faces a multi-state trial over the drivers' speculative claims.

It is also a victory for car manufacturers more broadly: as the Ninth Circuit emphasized in *Cahen*, nearly 100% of the cars on today's market feature wireless technology similar to the Uconnect system.

Had the *Flynn* case proceeded to trial, it could have opened the door to numerous other technology-based products liability actions founded on speculative threats of harm.

Taken together, the decisions in *Cahen* and *Flynn* suggest that courts are rightfully hesitant to allow claims of hypothetical injuries to shape cybersecurity jurisprudence.

Notes

[1] https://bit.ly/2W1XZYt

[2] https://bit.ly/3fhgPSV

[3] https://bit.ly/3dh4BrK

[4] https://bit.ly/3b4zC0y

This article first appeared on the Westlaw Practitioner Insights Commentaries web page on May 5, 2020.

ABOUT THE AUTHOR

Melissa DiGrande is a litigation associate at **Proskauer Rose LLP** in New York City. She focuses her practice on complex commercial litigation matters across a broad range of industries, including professional sports, lodging, pharmaceuticals and private equity. She can be reached at mdigrande@proskauer.com. This article was originally published April 7, 2020, on the firm's Minding Your Business Blog. Republished with permission.

Thomson Reuters develops and delivers intelligent information and solutions for professionals, connecting and empowering global markets. We enable professionals to make the decisions that matter most, all powered by the world's most trusted news organization.