Published on *The National Law Review* https://natlawreview.com

Fiat Chrysler Car Hacking Case Put In Neutral

Article By:

Securities and Capital Markets At Ballard Spahr

Plaintiff lawyers' continued search for damage theories to assert in claims arising from a data breach – or fear of a breach – received a potential setback this week when Chief Judge Michael Reagan of the United States District Court for the Southern District of Illinois permitted Fiat Chrysler and Harmon International to seek an interlocutory appeal of the court's earlier ruling in Flynn v. Fiat Chrysler US that class plaintiffs had standing to bring their "car hacking" claims in federal court. The ruling comes just one month before the scheduled start of trial. Fiat Chrysler and Harmon moved for an appeal after the Ninth Circuit ruled in a similar case, Cahen v. Toyota Motor Corp, that plaintiffs did not have standing to pursue diminution in value damages against Toyota based on a fear that the vehicles were susceptible to hacking.

Both Flynn and Cahen were filed in 2015, following a series of well-publicized demonstrations by white hat hackers that certain Toyota and Fiat Chrysler cars could be hacked and remotely controlled by a third party, in potentially malicious ways. Plaintiffs in both lawsuits asserted that the cybersecurity vulnerabilities that gave rise to the potential for hacking constituted a design defect that reduced the value of their cars.

The Ninth Circuit in Cahen previously rejected this diminution of value theory, agreeing with the District Court that "plaintiffs have not, for example, alleged a demonstrable effect on the market for their specific vehicles based on documented recalls or declining Kelley Bluebook values . . . nor have they alleged a risk so immediate that they were forced to replace or discontinue using their vehicles, thus incurring out-of-pocket damages." In rejecting Fiat Chrysler's motion to dismiss in the Flynn case, Judge Reagan reached a different conclusion, finding that plaintiffs had standing to seek diminution of value damages. Key to the court's decision was the fact that the cybersecurity defects in Chrysler cars that had been widely reported (originally in a Wired magazine article) led to a nationwide recall. The recall itself gave rise to additional reports of car hacking involving Chrysler cars, which the plaintiffs argued provided a foundation for a jury to conclude that the market value of Fiat Chryslers had been reduced. Additionally, plaintiffs alleged that the recall had not fixed the cybersecurity vulnerabilities, which the court found could give rise to a conclusion that the market for Chryslers had been altered.

In certifying the case for appeal, Judge Reagan explained that the initial finding of standing was debatable and noted that a ruling by the Seventh Circuit in favor of Fiat Chrysler would obviate the need for trial. The case remains stayed while the Seventh Circuit considers whether to agree to review the court's standing ruling.

A ruling by the Seventh Circuit rejecting the District Court's standing analysis in Flynn would potentially close what had been a new front in data breach litigation. Flynn had been one of only a few data security cases in the country to proceed past the motion to dismiss stage on a diminution in value theory of damages. What made Flynn particularly remarkable is that there had not been an actual reported breach that resulted in physical or other damages.

On the other hand, a ruling in favor of plaintiffs could have widespread ramifications and, in theory, could give rise to design defect claims against manufacturers of other connected products — such as refrigerators, medical devices, and smart televisions — based on data security vulnerabilities that increase the risk of hacking.

The Internet of Things is growing rapidly. According to Gartner, there are over 5 billion devices connected to the internet, and by 2020, there will be 25 billion, with revenues expected to exceed $300 billion. To be sure, there are important differences between the automobile market and the market for other consumer products that may limit the viability of overpayment damages claims for data security vulnerabilities outside of automobiles. Still, the potential that these IoT manufacturers could be subject to products liability claims stemming from cybersecurity vulnerabilities is an issue to watch carefully.

National Law Review, Volume VIII, Number 97