When a Cyberattack Might Be Espionage: DC Circuit Decides *In re U.S. Office of Personnel Management Data Security Breach Litigation*

July 19, 2019

By James P. Wehner

Reversing a dismissal at the district court level, the District of Columbia Circuit recently provided further clarity about when the risk of future harm is sufficient to provide standing in data breach cases when it revived some, but not all, data breach claims against the Office of Personnel Management and a government contractor. The case has particular relevance in circumstances in which a cyberattack may have been conducted or sponsored by a foreign government.

The OPM Breach

In 2013 and 2014, cyber attackers accessed the Office of Personnel Administration's network and accessed vast quantities of personal information relating to government employees, including 21.5 million background checks and 4 million federal employees' personnel files. These files included social security numbers and even fingerprints. Access to the database was accomplished by using credentials stolen from a contractor, KeyPoint Government Solutions, Inc.

District Court Proceedings

Numerous parties brought lawsuits, which were ultimately consolidated into two complaints in federal multidistrict litigation. The first was a putative class action brought by the American Federation of Government Employees on behalf of individuals affected by the breaches ("*Arnold*" case) alleging that OPM violated the Privacy Act by willfully failing to establish appropriate safeguards to ensure the security and confidentiality of their private information. It also brought a variety of common-law and statutory claims against KeyPoint, including negligence, negligent misrepresentation and concealment, invasion of privacy, breach of contract, and violations of the Fair Credit Reporting Act and state statutes. The second was an action for declaratory and injunctive relief brought by the National Treasury Employees Union ("*NTEU*" case) and three of its members.

At the district court, OPM and KeyPoint moved to dismiss both the *Arnold* case and the *NTEU* case arguing, among other things, that plaintiffs lacked Article III standing. Rejecting plaintiffs' argument that they faced a heightened risk of identity theft due to the breaches, the district court held that the facts alleged failed to plausibly support the conclusion that this risk of future injury was either substantial or clearly impending. The district court thus granted

both motions on the ground that neither the *Arnold* nor *NTEU* plaintiffs pled sufficient facts to demonstrate Article III standing.[1]

The Standing Analysis – Espionage and Identity Theft Are Not Mutually Exclusive

In 2017, the D.C. Circuit had held in *Attias v. Carefirst* that, because identity theft constitutes a concrete and particularized injury, whether a plaintiff has standing depends on whether the complaint plausibly alleges that the plaintiff faces "a substantial risk of identity theft" as a result of the defendants actions the data breach.[2] The D.C. Circuit there considered the nature of data stolen and the likely intent of the cyber attackers who obtained the data. In that case, involving a deliberate cyberattack, they found a substantial risk of identity theft. "No long sequence of uncertain contingencies involving multiple independent actors has to occur before the plaintiffs in this case will suffer any harm; a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken."[3]

Here, as in *Attias,* personal information was alleged to have been taken in a deliberate cyberattack. However, at the district court level the OPM had argued, and the district court had agreed, that the cyberattack here was insufficient to result in a "substantial risk" of identity theft because of reports that cyber attackers may have been Chinese government agents. Indeed the district court observed:

> Also, while this ruling is not based on the original complaints that were consolidated and amended in this multidistrict litigation, the Court notes that many of the plaintiffs specifically alleged that the breaches were widely reported to have been perpetrated by the Chinese government. . . . And, while the administration may have been officially circumspect at the time, possibly in light of the classified nature of the information, the state-sponsored nature of the attack was discussed publicly by some individual knowledgeable federal officials.[4]

On appeal, the D.C. Circuit found this reasoning improperly speculative, holding that:

---

1 *In re U.S. Office of Personnel Mgmt. Data Security Breach Litig*, 266 F. Supp. 3d 1, 38 (D.D.C. 2017), *aff'd in part*, *rev'd in part and remanded*, No. 17-5217, 2019 WL 2552955 (D.C. Cir. June 21, 2019). The district court also granted the motions to dismiss on several additional grounds beyond standing. *Id.* at 39-51.

2 *Attias v. Carefirst*, 865 F.3d 620, 627 (D.C. Cir. 2017).

3 *Id.* at 629.

4 *In re OPM*, 266 F. Supp. 3d at 33-34.

> [T]he district court should not have relied even in part on its own surmise that the Chinese government perpetrated these attacks. . . . Absent any factual allegations regarding the identity of the cyberattackers, the district court was not free to conduct its own extra-record research and then draw inferences from that research in OPM's and KeyPoint's favor.[5]

More importantly, the appellate court held that it was "just as plausible to infer that identity theft is at least one of the hackers' goals, even if those hackers are indeed affiliated with a foreign government."[6] As the court observed, "espionage and identity theft are not mutually exclusive."[7] The court distinguished these circumstances from ones in cases cited by OPM, including missing boxes or stolen laptops where there was some doubt that anyone had intentionally targeted personal information. Here, the plaintiffs alleged that the cyber attackers intentionally targeted their information.

The D.C. Circuit also addressed the time that had elapsed since the breach. While recognizing the general principle that as breaches "fade further into the past," threatened injuries become more speculative, the appellate court found that the two years between the attacks and the filing of the complaint was not enough to render the threat insubstantial. The court found in particular that the sophistication and scale of the attacks was a relatively new phenomenon, and "the passage of a year or two without any clearly identifiable pattern of identity theft or financial fraud means that all those whose data was compromised are in the clear."[8]

Conclusion

We can expect that courts will continue to evaluate risk of harm on a case-by-case basis. The D.C. Circuit's ruling in *In re OPM* is significant, however, in that it avoids creating a class of cyberattacks—state-sponsored or espionage-motivated cyberattacks—for which standing cannot be established. Speculation that a particular cyberattack was the work of a state actor would not foreclose recovery in a data breach action. In light of the increasing prominence of state-sponsored cyberattacks, this ruling will likely be important in future cases.

James P. Wehner is a Member of Caplin & Drysdale's Complex Litigation and Bankruptcy practice groups.

---

5 *In re U.S. Office of Personnel Mgmt. Data Security Breach Litig.*, 2019 WL 2552955, at *6.

6 *Id.* at *7.

7 *Id.*

8 *Id.* at *8.

Disclaimer
This communication neither provides legal advice, nor creates an attorney-client relationship with you or any other reader. If you require legal guidance in any specific situation, you should engage a qualified lawyer for that purpose. Prior results do not guarantee a similar outcome.

Attorney Advertising
It is possible that under the laws, rules, or regulations of certain jurisdictions, this may be construed as an advertisement or solicitation.