Risk of Harm Standing in Data Breach Cases - Latest Developments

02.09.2018 | Article
Lexology

Is an increased risk of harm sufficient to establish standing in a data breach case? Most courts have avoided an absolute answer, instead weighing the characteristics of the data breach. A recent New York case illustrates the difficulties courts have had with the question, while the Supreme Court considers an opportunity to clarify the answer.

Fero v. Excellus Health Plan

Just weeks ago, the U.S. District Court for the Western District of New York took a U-turn on risk of harm standing. In *Fero v. Excellus Health Plan, Inc.*, the court granted a motion for reconsideration and then denied defendants' motion to dismiss, which it had previously granted for lack of standing.[1]

Fero involves a healthcare provider, Excellus Health Plan. Plaintiffs allege that hackers gained access in 2013 to Excellus's computer systems and accessed names, birth dates, social security numbers, mailing addresses, phone numbers, and other medical insurance information.[2] Excellus moved to dismiss for lack of standing.[3] On February 22, 2017, the court concluded that certain plaintiffs "who did not allege that they had suffered any misuse of their personally identifiable information" failed to "allege an injury-in-fact based on the alleged harm of increased risk of identity theft."[4] The court thus granted the motion to dismiss as to those specific plaintiffs.[5]

Those plaintiffs then moved for reconsideration of the decision as to their claims and cited the Second Circuit's recent decision in *Whalen v. Michaels Stores, Inc.*, as an intervening change in controlling law that supported reconsideration.[6] In *Whalen*, the Second Circuit had affirmed an order of the district court which found that a plaintiff failed to allege a cognizable injury resulting from the exposure of her credit card information after a data breach at a Michaels store.[7] The Second Circuit agreed that the plaintiff failed to establish the "threat of future fraud" because her credit card was promptly cancelled and no other personally identifying information was allegedly stolen.[8] The *Fero* court concluded that the "implication" of the Second Circuit's language was that "had [the plaintiff] alleged the theft of personally identifying information, she would have had standing based on a threat of future fraud."[9] While concluding that *Whalen* "strongly implie[d]" that the Second Circuit would have found standing, it also reasoned that *Whalen* did not amount to a "change of controlling law" that would justify reconsideration under Rule 60(b).[10] Instead the court concluded that reconsideration of its dismissal order was warranted, in an exercise of its discretion, to avoid "manifest injustice."[11]

In the end, the *Fero* court reasoned that the Second Circuit would deem the theft of personally identifying information, such as social security numbers or birth dates, sufficient to confer standing on a risk of harm theory.[12]

Whether this is an accurate prediction of how the Second Circuit would calibrate risk of harm standing is, of course, speculative, but the *Fero* court is not alone in finding the question a challenging one. At the time of this writing, the Sixth, Seventh, Ninth, and D.C. Circuits have found standing based on the increased risk of identity theft while the Third, Fourth, and Eighth Circuits have not.[13] In most of these cases, however, the specific facts of each breach determine whether a risk of harm is real enough to confer standing. And the cases do not necessarily assess the facts in the same way. For example, some courts have taken into account costs incurred to avoid future harm,[14] while others, including the Eighth Circuit, have ruled out this fact as a basis for establishing injury in fact.[15]

Attias v. CareFirst

On February 16, 2018, the Supreme Court will decide whether to grant cert in *Attias v. CareFirst*, another case concerning the question of risk of harm standing.[16] If cert is granted, the Supreme Court will have the opportunity to provide clarity to litigants that seek to bring suit in the wake of data breaches that compromise their personal identifying information.

The *Attias* case stems from a 2014 data breach in which an unknown hacker gained access to CareFirst's, a health insurer, servers and stole names, birth dates, email addresses, and subscriber identification information for over one million policyholders.[17] These policyholders brought a proposed class action against CareFirst in the D.C. District Court alleging that CareFirst violated state laws and legal duties by failing to protect their personal information and exposing them to the risk of identity theft.[18]

The District Court held in favor of CareFirst and dismissed the complaint for lack of standing.[19] The court reasoned that the alleged injury was too speculative and that the mere fact that one's personal information was stolen in a data breach was insufficient to establish standing absent additional facts demonstrating a "sufficiently substantial risk of future harm."[20] On appeal, the D.C. Circuit reversed and held that the plaintiffs had plausibly alleged a risk of future injury that was substantial enough to confer Article III standing.[21] The D.C. Circuit explained that "the proper way to analyze an increased-risk-of-harm claim is to consider the ultimate alleged harm"—there, identity theft—"as the concrete and particularized injury and then to determine whether the increased risk of such harm makes injury to an individual citizen sufficiently 'imminent' for standing purposes."[22] Following this reversal, CareFirst petitioned the Supreme Court for certiorari.

CareFirst argues in its cert petition that the D.C. Circuit erroneously held plaintiffs to a "plausibility standard" and incorrectly interpreted the Supreme Court's "substantial risks" standard and related standing jurisprudence.[23] CareFirst also argues that the Court should grant cert to resolve the deepening circuit split over the issue.[24]

In opposition to the cert petition, Attias argues that a circuit split does not actually exist and that the differing outcomes in the circuit-level decisions can be explained by the substance of the underlying allegations in each case.[25] By way of example, Attias highlights the Eighth Circuit's decision in *SuperValu*, which rejected standing based largely on the fact that no personally identifying information such as social security numbers, birth dates, or driver's license numbers was stolen in the data breach.[26] In contrast, Attias argues, the D.C. Circuit was faced with differing factual allegations and a far more extensive loss of personal identifying information.[27] According to Attias, the courts are simply applying the same law to different factual allegations and there is nothing the Supreme Court need resolve.[28] Attias also contends that the D.C. Circuit correctly applied settled Supreme Court precedent regarding "imminent" injury.[29]

We will know soon whether the Supreme Court takes the opportunity to weigh in.

James P. Wehner is a Member of Caplin & Drysdale and Sally J. Sullivan is an Associate in the Firm's Complex Litigation practice group.

To view this article on *Lexology's* website, please visit this link (subscription required).

_____

[1] *Fero v. Excellus Health Plan, Inc.*, 6:15-cv-065659, 2018 WL 507320 (W.D.N.Y. Jan. 19, 2018).

[2] *Id*. at *2.

[3] *Id*. at *3.

[4] *Id*.

[5] *Id*. at *4.

[6] *Fero*, 2018 WL 507320 at *7.

[7] *Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89 (2d Cir. 2017)

[8] *Id*. at 90-91.

[9] *Fero*, 2018 WL 507320 at *10.

[10] *Id*. at *6.

[11] *Id*. at *10.

[12] *Id*. at *22.

[13] Compare *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384 (6th Cir. 2016) (finding standing based on increased risk of identity theft), and *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016) (same), and *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010) (same), and *Attias v. CareFirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017) (same), with *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011) (finding increased risk of identity theft insufficient for standing), and *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017) (same), and *In re SuperValu, Inc.*, 870 F.3d 763 (8th Cir. 2017) (same).

[14] *Galaria*, 663 F. App'x at 388 ("Plaintiffs' allegations of a substantial risk of harm, coupled with reasonably incurred mitigation costs, are sufficient to establish a cognizable Article III injury at the pleading stage of the litigation.").

[15] *In re SuperValu, Inc.*, 870 F.3d at 771 ("Because plaintiffs have not alleged a substantial risk of future identity theft, the time they spent protecting themselves against this speculative threat cannot create an injury.").

[16] Petition for Writ of Certiorari, *CareFirst, Inc. v. Attias*, No. 17-641, 2017 WL 5041488 (Oct. 30, 2017) (the "Petition").

[17] *Attias v. CareFirst, Inc.*, 199 F. Supp. 3d 193, 197 (D.D.C. 2016).

[18] *Id*.

[19] *Id*. at 202.

[20] *Id*. at 201.

[21] *Attias*, 865 F.3d 620.

[22] *Id*. at 627 (quoting *Public Citizen, Inc. v. Nat'l Highway Traffic Safety Admin.*, 489 F.3d 1279, 1298 (D.C. Cir. 2007)).

[23] Petition, *CareFirst*, 2017 WL 5041488, at *10.

[24] *Id*. at *10-15.

[25] Brief in Opposition to Petition for Writ of Certiorari, *CareFirst, Inc. v. Attias*, No. 17-641 (U.S. Jan. 2, 2018).

[26] *Id*. at 20-21.

[27] *Id*. at 21.

[28] *Id*. at 22-23.

[29] *Id*. at 6-15.

Attorneys

James P. Wehner
(202) 862-5075
jwehner@capdale.com

Related Practices/Industries

Complex Litigation