ROPES & GRAY ALERT

Privacy & Cybersecurity

September 27, 2017

Recent Decision Highlights Viability of Factual Challenges to Standing in Data Breach Cases

Private civil actions against companies that have suffered data security breaches raise a panoply of issues, but none more prevalent or decisive than those relating to injury and damages. This is because most plaintiffs in data security actions have not experienced any actual loss resulting from the breach, but instead premise their claims on alternative theories of injury, such as the risk of harm. Judicial decisions addressing data security claims have placed clear limitations on the types of injuries the law will remedy. One of those limits derives from the principle of standing, which asks whether plaintiff is the proper litigant to raise the breached company's alleged legal violations with the court. To have standing, a plaintiff must face an actual or sufficiently imminent future injury from the breach.

One way to challenge a plaintiff's standing is through a so-called "facial" challenge—that is, to argue the *complaint* fails to plausibly *plead* an actual or sufficiently imminent future injury from the breach. These facial challenges are frequently successful, but there have been exceptions. Accordingly, defendants should not overlook an additional, potentially powerful tool for attacking standing: a so-called "factual" challenge, which is based on evidence. Ropes & Gray recently highlighted a successful factual challenge to standing in a federal data breach case. A new decision from the Superior Court of Massachusetts, *Walker v. Boston Medical Center Corp. (BMC)*, SUCV201501733BLS1, 2017 WL 3612366 (Mass. Super. Ct. June 8, 2017), further underscores the viability of this approach.

Standing in Data Breach Litigation

Any private plaintiff in federal court bears the burden of demonstrating the "irreducible constitutional minimum of standing" under Article III of the U.S. Constitution—(1) an injury in fact; (2) caused by the defendant's conduct; (3) that is redressable by a favorable court decision.[1] The injury must be "actual or imminent, not conjectural or hypothetical."[2] Likewise, state courts frequently require that plaintiffs establish a sufficient injury in order to have standing to sue.[3]

The elements of standing "must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, *i.e.*, with the manner and degree of evidence required at the successive stages of the litigation."[4] Accordingly, "[a]t the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice," but "[i]n response to a summary judgment motion . . . the plaintiff . . . must set forth by

[1] *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560–61 (1992).
[2] *Id.* at 560 (internal quotation marks omitted).
[3] *See, e.g.*, La. Code Civ. Proc. Ann. art. 681; *Saratoga Cty. Chamber of Commerce, Inc. v. Pataki*, 798 N.E.2d 1047, 1052 (N.Y. 2003); *Pugsley v. Police Dep't*, 34 N.E.3d 1235, 1239–40 (Mass. 2015); *cf. Wexler v. Wirtz Corp.*, 809 N.E.2d 1240, 1243 (Ill. 2004) ("Under Illinois law, lack of standing is an affirmative defense."). Courts in all of these states have dismissed data breach suits for lack of standing. *See Bradix v. Advance Stores Co.*, NO. 2017–CA–0166, 2017 WL 3499012, at *3 (La. Ct. App. Aug. 16, 2017); *Manning v. Pioneer Sav. Bank*, 55 N.Y.S.3d 587, 593 (N.Y. Sup. Ct. 2016); *Maglio v. Advocate Health and Hosps. Corp.*, 40 N.E.3d 746, 756 (Ill. App. Ct. 2015); *Walker*, 2017 WL 3612366, at *4.
[4] *Lujan*, 504 U.S. at 561.

affidavit or other evidence specific facts," and, ultimately, controverted facts "must be supported adequately by the evidence adduced at trial."[5]

"Facial" challenges to consumers' standing in data breach cases—challenges that argue the complaint fails to plausibly plead an actual or imminent injury—have frequently been successful.[6] But there have been exceptions.[7] "Factual" challenges to standing—ones based on evidence—have also been successful at the motion-to-dismiss stage.[8] And, because standing in federal court is an issue of subject-matter jurisdiction, the parties in federal litigation may raise the issue throughout litigation (including for the first time on appeal),[9] and a court may consider the issue *sua sponte*.[10] If a challenge to standing fails early on, defendants should consider raising it again at later stages of litigation, when the plaintiff's burden only increases.[11]

How to Challenge Standing After the Motion-to-Dismiss Stage

To mount a factual challenge to standing after the motion-to-dismiss stage, a defendant can seek a preliminary pre-trial hearing on the question or raise the issue at trial.[12] Alternatively, the defendant can file a summary judgment motion.[13] In both federal and state court, defendants have successfully secured standing-based dismissals on summary judgment. *Walker*, a putative consumer class action alleging that defendants did not keep plaintiffs' medical information confidential, is a recent example. Defendant BMC used defendant MDF Transcriptions, LLC (MDF) to transcribe physicians' patient notes, which were available via MDF's online portal. Another customer of MDF inadvertently accessed a BMC transcription record. BMC subsequently notified all its patients whose records had been transcribed by MDF that there might have been unauthorized access to their medical information. Two of these patients then filed a putative class action against BMC and others.

---

[5] *Id*. (citations and internal quotation marks omitted).
[6] *See, e.g.*, *Beck v. McDonald*, 848 F.3d 262, 270–77 (4th Cir. 2017); *Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89, 90–91 (2d Cir. 2017); *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42–46 (3d Cir. 2011); *Allison v. Aetna, Inc.*, No. 09-2560, 2010 WL 3719243, at *3–7 (E.D. Pa. Mar. 9, 2010); *Amburgy v. Express Scripts, Inc.*, 671 F. Supp. 2d 1046, 1049–53 (E.D. Mo. 2009).
[7] *See, e.g.*, *Attias v. CareFirst, Inc.*, 865 F.3d 620, 625–29 (D.C. Cir. 2017) (rejecting facial challenge on ground that plaintiffs pleaded a sufficient risk of identity theft in the wake of the alleged theft of their personal information); *In re: Horizon Healthcare Servs. Inc. Data Breach Litig.*, 846 F.3d 625, 634–41 (3d Cir. 2017) (rejecting facial challenge on the ground that alleged violation of federal privacy statute resulting in disclosure of personal information to third party was sufficient for standing in data breach case) (citing *Spokeo, Inc. v. Robins*, 136 S.Ct. 1540 (2016)); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693–94 (7th Cir. 2015) (deciding that "it is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach," while noting "that the plaintiffs may eventually not be able to provide an adequate factual basis for the inference").
[8] *See Stapleton v. Tampa Bay Surgery Ctr., Inc.*, Case No: 8:17-cv-1540-T-30AEP, 2017 WL 3732102, at *1 n.1, *2–3 (M.D. Fla. Aug. 30, 2017) (construing standing challenge "[a]t the pleading stage" in data breach case "as a factual challenge to subject-matter jurisdiction" and dismissing complaint); *Foster v. Essex Prop. Inc.*, No. 5:14-cv-05531-EJD, 2017 WL 264390, at *2–4 (N.D. Cal. Jan. 20, 2017) (declarations submitted by defendant disproved any particularized and concrete injury, as well as causation between data breach and alleged harm).
[9] 13B Charles Alan Wright, Arthur R. Miller & Edward H. Cooper, Federal Practice and Procedure §3531.15 (3d ed. 2008).
[10] *Hinton v. Heartland Payment Sys., Inc.*, No. 09-594, 2009 WL 704139, at *1 (D.N.J. Mar. 16, 2009) (dismissing complaint sua sponte when plaintiff "fail[ed] to assert that he has suffered an actual or imminent injury in fact" as a result of a data breach).
[11] *See People To End Homelessness, Inc. v. Develco Singles Apartments Assocs.*, 339 F.3d 1, 8 (1st Cir. 2003) ("As litigation progresses, Article III places an increasingly demanding evidentiary burden on parties that seek to invoke federal jurisdiction. A plaintiff who has standing at the motion to dismiss stage, does not automatically have standing at the summary judgment or trial stage.").
[12] Charles Alan Wright, Arthur R. Miller & Edward H. Cooper, *supra* note 9.
[13] But, "if the ordinary summary-judgment rule is used to require the defendant, as moving party, to carry the burden of 'showing' at least that the plaintiff does not have evidence to carry the burden of proving facts that establish standing[,] [i]t is better" to challenge standing via a preliminary hearing, "as a means of requiring the plaintiff to carry its fact burden." Charles Alan Wright, Arthur R. Miller & Edward H. Cooper, *supra* note 9.

BMC moved to dismiss for, *inter alia*, lack of standing. The court, stating that the Massachusetts standard for standing is more relaxed than the federal one, "conclude[d] that the standing question should await a more full record and be decided upon a motion for summary judgment."[14]

On summary judgment, the court held that plaintiffs lacked standing to bring several state-law claims. Fatal to plaintiffs' claims was the failure to submit any evidence that an unauthorized person accessed plaintiffs' medical records—let alone that their records were misused—or that the public or even other MDF customers accessed BMC patient records. The mere possibility of unauthorized access was insufficient to confer standing.

The court rejected plaintiffs' argument that BMC's alleged failure to conduct a thorough investigation prevented plaintiffs from obtaining evidence of unauthorized access. The court emphasized that it was plaintiffs' "burden to present some evidence in the summary judgment record establishing harm or immediate risk of harm," "not BMC's responsibility to prove that the BMC records . . . were never accessed or misused by others,"[15] and noted that there was no evidence plaintiffs even tried to determine whether other MDF customers had similar improper access to patient records.

One named plaintiff argued that fraudulent tax returns were filed in her name, but the court held that, because a tax return requires a Social Security number, which was not contained in the plaintiff's transcriptions, the plaintiff failed to provide any evidence linking the fraudulent filings to her records at MDF.

Similarly, in *Hammond v. Bank of New York Mellon Corp.*, No. 08 Civ. 6060, 2010 WL 2643307 (S.D.N.Y. June 25, 2010), consumers brought a putative class action against a bank, alleging that the bank had stored their personal information on unencrypted tapes that were lost in transport. On defendant's motion for summary judgment pursuant to Federal Rule of Civil Procedure 56(c) and dismissal for lack of standing pursuant to Rule 12(b)(1), the court considered deposition transcripts and reports from proposed experts before concluding that plaintiffs' failure to "allege[] in the Complaint or adduce[] any evidence in discovery to suggest that their alleged injuries [were] more than 'speculative' or 'hypothetical' . . . [was] fatal to their standing."[16]

Data breach defendants can raise a variety of factual issues related to standing. To the extent plaintiffs claim they experienced or may experience misuse of their data or that they were forced to take steps to mitigate the risk of misuse, defendants can challenge whether plaintiffs' information was actually accessed or stolen, whether plaintiffs face a sufficiently imminent risk of loss from the access or theft, whether plaintiffs experienced any misuse of their data, whether they experienced any loss from the misuse, whether any misuse and/or loss is causally linked to the data breach suffered by the defendant, and whether and why plaintiffs took steps to mitigate the risk of misuse. To the extent plaintiffs allege that the value of their personal information was reduced by reason of the data breach, defendants can challenge the facts underlying that claim as well—for instance, by showing that plaintiffs have never even tried to sell their personal information, that they were never forced to accept a lower price in doing so because of the breach, or that the data never even had the value plaintiffs claim it did in the first place. Likewise, to the extent plaintiffs claim that they lost the benefit of a "bargain" they had struck with defendant in which defendant promised to adequately safeguard plaintiffs' data, defendants can show that, for instance, there was no such bargain over data

[14] *Walker v. Boston Med. Ctr. Corp.*, No. SUCV20151733BLS1, 2015 WL 9946193, at *1 & n.4 (Mass. Super. Ct. Nov. 20, 2015) ("How 'real and immediate' the risk of harm is should be evaluated when the facts surrounding the data breach, including the quantity and nature of access to the records, are presented after discovery.").
[15] *Walker*, 2017 WL 3612366, at *3.
[16] *Hammond*, 2010 WL 2643307, at *8; *see also Beck*, 848 at 270–77 (affirming both facial and factual standing challenges in consolidated data breach appeals, one on the pleadings and one on summary judgment). The *Hammond* court went on to note that named plaintiffs' lack of standing could "undermine" their status as lead plaintiffs. *Hammond*, 2010 WL 2643307, at *8 n.11. Defendants may have compelling standing-based challenges to class certification, a topic beyond the scope of this article.

security. In short, all options are on the table in a factual challenge—and as *Walker* demonstrates, success can mean full dismissal of the litigation.

For more information regarding the *Walker* decision or to discuss data security practices generally, please feel free to contact Rohan Massey, Doug Meal, Heather Egan Sussman, Jim DeGraw, Seth Harrington, Mark Szpak, Michelle Visser, David Cohen, Jen Walker or another member of Ropes & Gray's leading privacy & data security team.