Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Lack Of Standing — Data Breach Defense In State Court Too

Law360, New York (August 07, 2014, 10:24 AM ET) --

John Nadolenco

While data privacy — especially data breach — cases in the United States have been on the rise for years now, most cases never make it past the pleading stage. Indeed, federal courts frequently dismiss data privacy complaints for lack of standing under Article III of the U.S. Constitution — i.e., injury in fact. Article III has become the first (and often last) line of defense for companies accused of improperly collecting or protecting consumer data, particularly given the high costs of discovery and potential exposure in such cases.

Of course, not all claims arise under federal law or are subject to removal to federal court. State data privacy defendants are not without recourse, however. As several recent decisions show, the principles underlying an Article III defense often also apply under state law, especially where injury is an element of many statutory and common law claims.

The U.S. Supreme Court has long interpreted the Constitution's "case or controversy" provision to require (1) concrete and particularized injury in fact that is (2) fairly traceable to the defendant's conduct and is (3) capable of redress by judicial decision.[1] In 2013,in Clapper v. Amnesty International, the court held that a threat of future surveillance was "too speculative" to satisfy Article III, even though the plaintiffs allegedly had incurred costs, such as international airfare, to keep their communications private.[2]

Since Clapper, and even before, numerous federal courts have dismissed class actions alleging data collection and/or breach, but not data dissemination or misuse.[3] The principles that underlie these dismissals are not necessarily limited to Article III standing analysis, as recent decisions from Illinois and California show.

The Illinois cases began when burglars stole four laptops from Advocate Health and Hospitals, a network of affiliated doctors and hospitals. An Advocate patient, Veronica Vides, brought suit in state court, alleging that Advocate failed to encrypt and protect the laptops, subjecting patients to increased risk of identity theft, out-of-pocket costs to mitigate the risk and anxiety.[4] Vides predicated her claims on several Illinois statutes — the Consumer Fraud and Deceptive Business Practices Act, the Personal Information Protection Act and the Consumer Fraud Act — as well as common law negligence, invasion of privacy and infliction of emotional distress. Vides sought damages on behalf of all Advocate patients

treated prior to the theft.

The circuit court, citing Clapper and numerous federal cases, dismissed Vides' class action complaint with prejudice.[5] According to the court, the threat of identity theft depended on a "chain of attenuated and hypothetical events" including "whether [patient] data was actually taken after the removal, whether it was subsequently sold or otherwise transferred, whether anyone who obtained the data attempted to use it, and whether or not they succeeded."

To establish standing, the court concluded, the risk of identify theft need not be "literally certain," but must be "imminent" or "certainly impending." As in Clapper, costs incurred to offset such risks were insufficient; otherwise, plaintiffs could "manufacture standing merely by inflicting harm on themselves." A month after Vides, a second Illinois circuit court reached the same conclusion in Maglio v. Advocate Health & Hospitals Corp., dismissing another Advocate patient's class action with prejudice for failure to allege standing.[6]

Similarly, a Los Angeles judge recently dismissed claims that Ralphs Grocery Company disclosed to trusted business partners customer information obtained through its free rewards program. The California Court of Appeal affirmed, in an unpublished decision, holding that plaintiff Jacob Heller lacked standing to assert claims under California's Unfair Competition Law , which requires injury in fact.[7] Heller alleged that he would not have applied for the rewards card or shopped at Ralphs, had he known about the information sharing, and he sought disgorgement of profits on behalf of all Ralphs rewards members.

What was "notably missing" from Heller's complaint, however, was any economic injury resulting from his use of the rewards card. "The card was provided without cost," and there was no allegation "that any product purchased was not as represented." This failure was sufficient to defeat Heller's claims under the UCL and for breach of contract, fraud, intentional misrepresentation and negligence.

On the other hand, in Tabata v. Charleston Area Medical Center Inc., the West Virginia Supreme Court reversed a circuit court decision refusing to certify claims that a medical center inadvertently published patient information on the Internet.[8] The state supreme court "agreed with the circuit court that the risk of future identity theft alone does not constitute an injury in fact for the purpose of showing standing," but found that patients had a "concrete, particularized, and actual" interest "in having their medical information kept confidential," even though discovery revealed that the patient data had not yet been accessed on the internet.

Tabata is arguably best read as an outlier, distinguishable in that it allegedly involved actual — albeit accidental — dissemination of patient data by the defendant (as opposed to a data thief) and special state law duties imposed on doctors. Moreover, the Maglio court expressly addressed Tabata, and found that federal cases "more persuasively analyze" the standing issue.

Businesses should be aware of Tabata, nonetheless, particularly health care providers and companies operating in West Virginia. Ralphs and Advocate, meanwhile, reinforce the prevailing rule that increased risk of identity theft, without more, is often not enough to establish standing in state or federal court.

—By John Nadolenco and Evan Wooten, Mayer Brown LLP

John Nadolenco is a partner and Evan Wooten is an associate in Mayer Brown's Los Angeles office.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992).

[2] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143 (2013).

[3] See, e.g., In re SAIC Backup Tape Data Theft Litig., No. 12-cv-0347 (JEB) (D.D.C. 2014); Galaria v. Nationwide Mutual, No. 2:13-cv-118 (S.D. Ohio 2014); In reBarnes & Noble, No. 1:12-cv-08617 (N.D. Ill. 2013). But see In re Sony Gaming Networks, 3:11-md-02258,(S.D. Cal. 2014) ("credible threat" that compromised data could be accessed by third parties was sufficient to satisfy Article III).

[4] Vides v. Advocate Health & Hosps. Corp., No. 13-CH-2701 (Ill. 19th Judicial Cir. May 27, 2014).

[5] Illinois employs a standing analysis similar to the federal standard: "distinct and palpable" injury, fairly traceable to the defendant's conduct and redressible by court action. Greer v. Ill. Hous. Dev. Auth., 122 Ill. 2d. 463, 492-93 (1988).

[6] Maglio v. Advocate Health & Hosps. Corp., No. 13-CH-2701 (Ill. 16th Judicial Cir. July 10, 2014).

[7] Heller v. Ralphs Grocery Co., No. B249608 (June 23, 2014).

[8] Tabata v. Charleston Area Med. Ctr. Inc., No. 1301799 (W. Va. May 28, 2014).
