AN A.S. PRATT PUBLICATION
JANUARY 2017
VOL. 3 • NO. 1

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 3 | NUMBER 1 | JANUARY 2017

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3000
Fax Number .... (518) 487-3584
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3000

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [297] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2017–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 718.224.2258. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Data Breach Class Action Lawsuits: First Response for Defense – Motion to Dismiss for Lack of Standing

By James M. Westerlind and Malcolm McNeil*

When faced with a data breach class action alleging that plaintiffs have suffered an increased risk of future identity theft, companies should consider responding to the complaint by filing a motion to dismiss under Rule 12(b)(1) of the Federal Rules of Civil Procedure for lack of subject matter jurisdiction on the ground that the putative class action plaintiffs lack standing to sue. The authors of this article explain the reason for this suggested response and the growing split among the Circuit courts on this issue.

Nearly every state and territory in the U.S. requires a company that has, or reasonably believes that it has, experienced a data breach that may involve the compromise of the personal identifiable information of its customers to notify those individuals promptly. After such a notice has been sent by a company, there is often a race to the courthouse by the plaintiffs' bar to be the first (and lead) counsel in a class action lawsuit against the company. Rather than waiting to identify customers who have actually experienced identity fraud that was likely caused by the data breach, in their zeal to be first, plaintiffs' counsel often files a putative class action complaint naming a handful of plaintiffs who have not experienced identity theft. Rather, the complaint alleges that the plaintiffs have suffered an *increased risk of future* identity theft and that they should be able to recover costs that they have incurred to mitigate that risk of future harm. The company should respond to a complaint containing such allegations by filing a motion to dismiss under Rule 12(b)(1) of the Federal Rules of Civil Procedure for lack of subject matter jurisdiction on the ground that the putative class action plaintiffs lack standing to sue.

ARTICLE III STANDING

The "case or controversy" language of Article III of the U.S. Constitution requires each plaintiff who files a complaint in federal court to have standing to pursue each claim asserted. If the plaintiff lacks standing to sue, the federal court lacks subject matter jurisdiction to decide the case and must dismiss the complaint without prejudice.

* James M. Westerlind is counsel in Arent Fox LLP's litigation, insurance, cybersecurity and data protection, and automotive practice groups. Malcolm McNeil is a partner at the firm, where he focuses on litigation, business, cybersecurity and data protection, and transactional matters involving international clients. They authors may be reached at james.westerlind@arentfox.com and malcolm.mcneil@arentfox.com, respectively.

If the defendant moves to dismiss the complaint for lack of standing, the plaintiff has the burden of establishing the following elements: (1) *injury-in-fact*, which is an invasion of a legally protected interest which is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical; (2) *causation*, in that the alleged injury must be fairly traceable to the challenged action of the defendant; and (3) *redressability*, meaning that it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.[1] The motion to dismiss can proceed as a facial challenge, meaning that the defendant asserts that the allegations of the complaint are insufficient to establish standing, or a factual challenge, where the defendant submits evidence that the jurisdictional allegations of the complaint are untrue. In a putative class action, any named plaintiff must allege that he or she has been personally injured by the alleged wrongful conduct of the defendant. A named plaintiff cannot rely on injuries allegedly sustained by unknown and unidentified class members.[2]

Where a plaintiff alleges that he or she will suffer future harm as a result of the defendant's purported wrongful conduct, as opposed to alleging that he or she has already suffered actual injury, the alleged future harm must be "certainly impending" to constitute injury-in-fact,[3] or there must be a "substantial risk" that harm will occur.[4] Allegations of *possible* future injuries are insufficient. And where the alleged injury requires a lengthy chain of inferences, courts typically conclude that there is no injury-in-fact. Moreover, where the alleged injury is contingent on the decisions and actions of unknown third-parties, courts generally decide that there is no injury-in-fact.

Most of the data breach class action lawsuits that have been filed over the past few years have alleged that the data breach only increased the likelihood that the named plaintiffs and the putative class members may be victims of identity theft in the future. Few named plaintiffs have alleged that they suffered actual identity theft. And if actual identity theft is alleged, it still must be fairly traceable to the subject data breach and the harm must be redressable.

CAUSATION: FAIRLY TRACEABLE

In re Science Applications Int'l Corp. Backup Tape Data Theft Litig. ("*SAIC*"),[5] is a good example of a case where the "fairly traceable" element was applied. In *SAIC*, a thief broke a window in the defendant's employee's car and stole the stereo, a GPS and data tapes. The data tapes contained the medical records for 4.7M military families enrolled in TRICARE. The data on the tapes included names, social security numbers,

[1] *See Lujan v. Defenders of Wildlife*, 504 U.S. 555 (1992).
[2] *See Simon v. E. Ky. Welfare Rights Org.*, 426 U.S. 26 (1976).
[3] *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013).
[4] *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334 (2014).
[5] 45 F. Supp. 3d 14 (D. D.C. 2014).

addresses, dates of birth, phone numbers and medical information. But no financial data, such as credit card or bank account information, were on the data tapes. Only two named plaintiffs alleged actual injury; the rest of the named plaintiffs were dismissed because they alleged only the increased risk of future harm.

Of the two plaintiffs who alleged actual harm, one alleged that a bogus loan application had been submitted to American Express in his name. The information used for the loan application was on the stolen data tapes, so this plaintiff had standing to sue. But the court noted that the plaintiff had alleged a spate of other identity attacks against him that used personal information that was not on the tapes.

The other plaintiff alleged that she had received unsolicited calls from medical companies on her unlisted telephone number for a medical condition that was in the stolen tapes. The unlisted telephone number was in the tapes also. Therefore, since there was a credible link between data on the stolen tapes and the alleged injury, this plaintiff had standing to sue.

An example of a case where the court used the "fairly traceable" element to dismiss a case where actual identity theft was alleged is *In re Horizon Healthcare Services Inc. Data Breach Litig.*[6] In that case, a thief stole two laptops containing unencrypted personal identifiable information for more than 839,000 members of the defendant healthcare company, including names, addresses, member I.D. numbers, dates of birth, and, for some, social security numbers and clinical information. Only one named plaintiff alleged actual identity theft. Specifically, he alleged that a fraudulent tax return had been filed under both his and his wife's name. But since the wife's personal information was not in the stolen laptops, the court concluded that this alleged harm was not fairly traceable to the data breach. Further, the court concluded that since this plaintiff had received the tax refund, the harm was not redressable.

This same plaintiff also alleged that his credit card had been misused. But since his credit card information was not in the stolen laptops, this harm was also not fairly traceable to the data breach.

TYPES OF FUTURE HARM TYPICALLY ALLEGED

Increased Risk of Identity Theft

The first and most common type of future harm that has been alleged by plaintiffs in data breach lawsuits is the increased risk of future harm. But this type of alleged injury is usually dismissed because there are often too many assumptions required to show that harm is "certainly impending." That is, there are too many "ifs."

[6] No. 13-cv-7418 (CCC) (D. N.J. Mar. 31, 2015).

As noted by the court in *SAIC*, the thief would have to:

- recognize the data tapes that he stole for what they were;
- find a tape reader and attach it to the stolen device;
- acquire software to upload the data from the tapes onto a computer;
- decrypt those portions of the data that were encrypted;
- acquire familiarity with TRICARE's database format (which may require additional software); and
- either misuse a plaintiff's personal identifiable information or sell it to a willing buyer who would then misuse it.

Since many of these "ifs" would be dependent on the actions of unknown third-parties, the court concluded that they could not be considered for establishing injury-in-fact for standing.[7]

Mitigation Expenses

Many plaintiffs in data breach lawsuits allege that they had to purchase credit-monitoring services and that they incurred additional expenses in obtaining replacement accounts and credit and debit cards, and that these reasonably incurred mitigation expenses should be sufficient to satisfy the injury-in-fact element of standing. Most courts have held that mitigation expenses satisfy the injury-in-fact element of standing if the plaintiff has also alleged actually injury that is fairly traceable to the subject data breach. However, most courts to address this argument where the plaintiffs only allege an increased risk of future harm have held that, absent a plausible showing that the alleged future harm is "certainly impending" or a "substantial risk," a plaintiff cannot manufacture standing by choosing to make expenditures based on a hypothetical harms, no matter how reasonable those mitigation efforts may be.[8]

Loss of the Benefit of the Bargain

Some data breach lawsuit plaintiffs include a contractual claim, alleging that the price that they paid to the defendant for their health insurance, product, services, etc. included data protection services, and that since the defendant failed to provide those data protection services, the plaintiffs over-paid the defendant. This claim is a spin-off of a product liability theory adopted by some courts where the product itself was alleged to be defective or dangerous and the consumers claimed that they would not have purchased the product (or paid a premium for it) had they known of the defect. Most courts to have confronted this claim in the data breach context have dismissed it.[9] Moreover, the plaintiffs often fail to plausibly allege: (1) that the value of the goods or services they purchased was diminished as a result of the data breach; (2) how the

[7] *SAIC*, 45 F. Supp. 3d at 25-26 (citing *Clapper*, 133 S. Ct. at 1150)).

[8] *See, e.g., Attias v. CareFirst, Inc.*, No. 15-cv-0082 (CRC)(D. D.C. Aug. 10, 2016); *Chambliss v. CareFirst, Inc.*, No. 15cv-2288 (RDB)(D. Md. May 27, 2016).

[9] *See, e.g., Lewert v. P.F. Chang's Bistro, Inc.*, 819 F.3d 963, 968(7thCir. 2016); *SAIC*, 45 F. Supp. 3d at 30 (holding that theory "too flimsy" to support standing).

price they paid for data protection was incorporated into the price they paid for the products or services (*i.e.*, they fail to quantify their alleged losses); and (3) that the defendant understood that data protection was included in the purchase price (as a contractual theory must allege a meeting of the minds between the parties).

Statutory Violations

Some plaintiffs allege that the defendant violated various consumer protection statutes in connection with the data breach, and that such violations cause injury *per se* or the statutes themselves set a damage amount per violation, which satisfies the injury-in-fact element of standing. Plaintiffs' arguments here appear to conflict with the U.S. Supreme Court's most recent decision on the subject of standing in *Spokeo, Inc. v. Robins*.[10] In *Spokeo*, the Court reiterated that Congress cannot erase Article III's standing requirements by statutorily granting the right to sue to a plaintiff who would not otherwise have standing. A statute concerns the particularization, but not the concreteness, of alleged injury, and "Article III standing requires a concrete injury even in the context of a statutory injury."[11] And a concrete injury must be *de facto*; *i.e.*, it must actually exist.[12] Where a statutory violation may result in no harm, the mere violation is insufficient to confer standing.[13]

Loss of Value of Personally Identifiable Information

A number of data breach plaintiffs have also alleged that the data breach has decreased the value of their personally identifiable information, and that these allegations are sufficient for standing. The courts have generally rejected this theory, primarily because the plaintiffs have not alleged that they intended to sell their personal information on the cyber black market, and the plaintiffs usually fail to allege how their personal information has been devalued by the breach.[14]

CASES WHERE COURTS HAVE HELD THAT ALLEGATIONS OF FUTURE HARM ARE SUFFICIENT FOR STANDING

The most favorable jurisdictions for data breach class action plaintiffs are in the U.S. Courts of Appeal for the Seventh, Ninth, and, most recently, Sixth Circuits. Last September, the Sixth Circuit Court of Appeals reversed the Southern District of Ohio's ruling that the plaintiffs' initial putative class action complaint failed to allege injury-in-fact because no actual harm, rather only the increased of future

[10] 136 S. Ct. 1540 (2016).

[11] *Spokeo*, 136 S. Ct. at 1549.

[12] *Id.* at 1543.

[13] *See Attias, supra*; *see also Hancock v. Urban Outfitters, Inc.*, No. 14-cv-7047 (D. D.C. Jul. 26, 2016) (plaintiffs' claims that defendant retailers violated D.C. statutes by requesting ZIP codes with credit card purchases failed to allege concrete injury-in-fact; violations of statute alone insufficient for standing).

[14] *See, e.g., Attias, supra*; *SAIC*, 45 F. Supp. 3d at 29-30.

harm, was alleged.[15] The Sixth Circuit concluded that the plaintiffs' allegations were sufficient because "[t]here is no need for speculation where Plaintiffs allege that there data has already been stolen and is now in the hands of ill-intentioned criminals."[16] But this rationale appears to violate the well-settled standing rule that where alleged future injury is contingent on the decisions and actions of unknown third-parties, there is no injury-in-fact. [17]

Moreover, the Sixth Circuit's reliance on the Seventh Circuit's decisions in *Remijas v. Neiman Marcus Group, LLC*,[18] and *Lewert v. P.F. Chang's China Bistro, Inc.*,[19] and the Ninth Circuit's decision in *Krottner v. Starbucks Corp.*,[20] is suspect. In *Remijas*, 9,200 of the 350,000 customers of Neiman Marcus whose personal identifiable information was stolen had experienced identity theft. In *Lewert*, a named plaintiff had experienced fraudulent charges on the credit card that he had used at P.F. Chang's. Hence, the Seventh Circuit cases are distinguishable. And *Krottner* is a pre*Clapper* decision, which pre-dates the Supreme Court's strong emphasis and reiteration in 2013 that alleged future injury must be "certainly impending" to satisfy injury-in-fact.

The Sixth Circuit also noted that the plaintiffs had cited to a study showing that in 2011, recipients of data breach notifications were 9.6 times more likely to experience identity fraud, and had a fraud incidence rate of 19 percent.[21] The majority of courts have rejected these statistic arguments because "the degree by which the risk of harm has increased is irrelevant – instead, the question is whether the harm is certainly impending."[22] Indeed, in *Strautins v. Trustwave Holdings, Inc.*,[23] the plaintiffs had cited to a similar 2012 study that showed that victims of a data breach were 9.5 times more likely to be victims of identity theft in the future. The court noted that the same study also stated that only 25 percent of data breach victims actually experience identity fraud which, if true, meant that 75 percent of data breach victims never experience identity fraud. The *Strautins* court held that such a risk is not "certainly impending."[24]

---

[15] *See Galaria/Hancox v. Nationwide Mut. Ins. Co.*, Nos. 15-3386/3387 (6th Cir. Sep. 12, 2016).
[16] *Id.*
[17] *See Clapper*, 133 S. Ct. at 1150; *see also Simon v. E. Ky. Welfare Rights Org.*, 426 U.S. 26 (1976).
[18] 794 F.3d 688 (7th Cir. 2015).
[19] 819 F.3d 963 (7th Cir. 2016).
[20] 628 F.3d 1139 (9th Cir. 2010).
[21] *See Galaria/Hancox, supra.*
[22] *SAIC*, 45 F. Supp. 3d at 25.
[23] 27 F. Supp. 3d 871 (N.D. Ill. 2014).
[24] *Strautins*, 27 F. Supp. 3d at 877; *see also SAIC*, 45 F. Supp. 3d at 32 ("In a society where around 3.3% of the population will experience some form of identity theft – regardless of the source – it is not surprising that at least 5 people out of a group of 4.7 million happen to have experienced some form of credit or bank account fraud.") (citation omitted).

CONCLUSION

A company served with a complaint seeking damages premised on a data breach that the company has experienced should consider moving to dismiss the complaint for lack of standing. If the plaintiffs only allege the risk of future identity theft, as opposed to actual identity theft, the defendant will likely have a strong argument that the plaintiffs lack standing to sue. While the Seventh, Ninth, and Sixth Circuits have held that the allegations of future harm in those particular cases were sufficient to confer standing at the pleading phase, those decisions may be distinguishable on their facts from your company's situation. And, in *Remijas*, the Seventh Circuit indicated that it was unlikely that the plaintiffs other alleged injuries – (1) overpayment for products, (2) loss of value of personal information, and (3) statutory violations (specifically, violations of breach notification statutes) – would likely satisfy the injury-in-fact element of standing.[25]

Further, the U.S. Supreme Court has addressed the issue of standing on no less than three separate occasions over the past three years – *Clapper* (2013), *Driehaus* (2014), and *Spokeo* (2016) – and in each instance has reversed the Circuit court's decision finding standing based on the Court's prior-stated standing principles. That is, the U.S. Supreme Court does not seem inclined to expand the scope of standing, and it may very likely in the near future grant *certiorari* of an appeal in a data breach standing case to clarify the law in this regard and put an end to the growing split among the Circuit courts.

[25] *Remijas*, 794 F.3d at 695-96.