AN A.S. PRATT PUBLICATION
NOVEMBER – DECEMBER 2017
VOL. 3 • NO. 9

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 3 NUMBER 9 NOVEMBER/DECEMBER 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) 487-3385
Fax Number .... (800) 828-8341
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 ..... (937) 247-0293

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 [303] (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.

With Equifax Looming, Split on Standing in Data Breach Cases Grows with Recent Decisions

By Jonathan S. Kolodner, Rahul Mukhi, and Tanner Mathison*

The authors of this article discuss several recent decisions that have widened a split on when and under what conditions customers or other affected individuals may bring claims against a company that suffers a data breach.

As the Equifax breach litigation gets underway, several recent decisions have widened a split on when and under what conditions customers or other affected individuals may bring claims against a company that suffers a data breach. Recently, a D.C. federal judge dismissed a lawsuit based on the massive breach at the U.S. Office of Personnel Management ("OPM"), ruling that the theft of data alone was not enough to establish standing. The U.S. Court of Appeals for the Eighth Circuit issued a similar recent ruling, holding that plaintiffs suing the grocery retail company SuperValu had not shown that they were at greater risk of identity theft as a result of a data breach at the company and they therefore lacked standing.

In contrast to these decisions, a California federal judge allowed claims to proceed against Yahoo! based on the allegation that the customer-plaintiffs alleged a risk of future identity theft and loss of value of their personal identification information.

The differing interpretations of the standing requirements in data breach cases will no doubt continue to be vigorously litigated and may ultimately need to be resolved by the U.S. Supreme Court.

BACKGROUND: THE DATA BREACHES

The recent decisions arise from three different data breaches at OPM, SuperValu, and Yahoo!:

- In June 2015, federal officials announced that OPM had been the target of a data breach targeting millions of people, including government employees and others. According to numerous reports, the attack originated in China and the FBI arrested a Chinese national connected to the malware used in the breach.

* Jonathan S. Kolodner is a partner and Rahul Mukhi is counsel at Cleary Gottlieb Steen & Hamilton LLP focusing their practices on criminal, securities, and other enforcement and regulatory matters as well as on complex commercial litigation. Tanner Mathison is a law clerk at the firm concentrating on litigation and enforcement matters. The authors may be contacted at jkolodner@cgsh.com, rmukhi@cgsh.com, and tmathison@cgsh.com, respectively.

- In 2014, unknown computer hackers accessed SuperValu's payment processing systems and gained access to customer names and credit card information. SuperValu disclosed the breach shortly thereafter.
- Between 2013 and 2016, Yahoo! suffered three massive data breaches. Yahoo! originally disclosed the attacks in late 2016 and recently announced that the breach was bigger than initially described, potentially affecting all three billion of its accounts.

As has become increasingly common, on the heels of the disclosure of each of these breaches, plaintiffs' law firms promptly brought claims on behalf of customers against the companies. The plaintiffs alleged violations of state consumer protection laws, breach of contract, and common law negligence and claimed that their heightened risk of identity theft, among other alleged injuries, was sufficient to establish standing.

In the recent cases involving OPM, SuperValu, and Yahoo!, one court agreed with plaintiffs that they had established standing, while the other two courts agreed with the defendants and dismissed the cases.

THE GROWING SPLIT ON STANDING REQUIREMENTS

The standing requirement under Article III of the U.S. Constitution limits federal court jurisdiction to actual cases and controversies. Under the Supreme Court's most recent standing decision, in a case called *Spokeo*, plaintiffs must allege a "concrete and particularized" injury that is "actual or imminent, not conjectural or hypothetical."[1] Multiple circuits have held that exposure of consumers' data to potential identity theft is sufficient to establish Article III standing.[2] While at least two circuits have held the opposite.[3]

The *OPM* Decision

In the OPM litigation, the U.S. District Court for the District of Columbia held that plaintiffs had not pled an actual injury beyond the mere theft of their data, which it found was insufficient to establish Article III standing.[4] The court distinguished the OPM breach from breaches of retail companies, which the court believed could support an inference that hackers obtained information to make fraudulent charges

[1] *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016).

[2] *See e.g., Attias v. CareFirst Inc.*, 865 F.3d 620 (D.C. Cir. 2017); *Galaria v. Nationwide Mut. Ins. Co.*, No. 15-3386, 2016 (6th Cir. Sept. 12, 2016); *Resnick v. AvMed, Inc.*, 693 F.3d 1317 (11th Cir. 2012).

[3] *See Whalen v. Michaels Stores, Inc.*, 689 Fed. Appx. 89 (2d Cir. May 2, 2017); *Beck v. McDonald*, 848 F.3d 262, 268 (4th Cir. 2017), cert. denied sub nom. *Beck v. Shulkin*, No. 16-1328 (U.S. June 26, 2017).

[4] *In re: U.S. Office of Personnel Management Data Security Breach Litigation*, Misc. Action No. 15-1394 (ABJ), MDL Docket No. 2664 (D.D.C. Sept. 19, 2017).

or commit identify theft.[5] The court found that such assumptions did not apply in the OPM breach context, which involved the theft of government employee information potentially by Chinese nationals. Even for the plaintiffs who did allege that they had already experienced an actual misuse of their credit card numbers or personal information, the court held that they could not tie those disparate incidents to the OPM breach. Accordingly, the court dismissed the case for lack of standing.

The *SuperValu* Decision

In the SuperValu case, plaintiffs who had their credit card information stolen relied on a 2007 Report from the Government Accountability Office (the "2007 GAO Report") to support their "otherwise bare [standing] assertion that '[d]ata breaches facilitate identity theft.'"[6] The court reasoned that because the stolen credit card information could not be used to open new accounts, the only possible risk to the plaintiffs was credit card fraud. However, the 2007 GAO Report relied on by the plaintiffs also stated that "most breaches have *not* resulted in detected incidents of identity theft."[7] For these reasons, the Eighth Circuit held that the plaintiffs' allegations did "not plausibly support the contention that consumers affected by a data breach face a *substantial risk* of credit or debit card fraud," and thus did not establish standing under *Spokeo*. Nevertheless, in a footnote, the court stated, "[w]e recognize there may be other means—aside from relying on reports and studies—to allege a substantial risk of future injury, and we do not comment on the sufficiency of such potential methods here."[8]

The *Yahoo!* Decision

In contrast to these two decisions, the District Court for the North District of California allowed plaintiffs' claims to proceed against Yahoo! Among other things, the court held that the alleged "risk of future identity theft" and the loss of value of personal identifying information were sufficient injuries to justify the plaintiffs' standing to bring suit.[9] In doing so, the court relied on the U.S. Court of Appeals for the Ninth Circuit's decision *In re Facebook Privacy Litigation*,[10] which found that the plaintiffs plausibly alleged that they experienced harm where the plaintiffs' personal information was disclosed in a data breach and they therefore "los[t] the sales value of

---

[5] The court distinguished *Attias v. CareFirst Inc.*, 865 F.3d 620 (D.C. Cir. 2017), where the D.C. Circuit held that plaintiffs had established standing based on claims that their information was stolen from a health insurance company.

[6] *In re: SuperValu, Inc.*, *Customer Data Security Breach Litigation*, 16-2378 Slip Op. at 10-11 (Aug. 30, 2017).

[7] 2007 GAO Report at 21 (emphasis added).

[8] *In re: SuperValu, Inc.*, *Customer Data Security Breach Litigation*, 16-2378 Slip Op. at 10-11 (Aug. 30, 2017).

[9] *In Re: Yahoo! Inc. Customer Data Security Breach Litigation*, 16-MD-02752-LHK: 94 (Aug 30, 2017).

[10] 72 F. App'x 494, 494 (9th Cir. 2014).

th[eir] [personal] information." Thus, the *Yahoo!* and *Facebook* decisions are in tension with the two other recent decisions outside of the Ninth Circuit discussed above, which held that similar allegations did not establish Article III standing in those cases.

TAKEAWAYS

With a growing number of courts coming to different outcomes on the viability of data breach litigation, it is likely that these issues will continue to be at the forefront of breach litigation cases, including in the Equifax consumer cases. Data breach plaintiffs will likely seek to marshal as much factual support for their allegations of heightened risk of injury and, if they are able, actual injury caused by the breach. This will likely turn on the types of data compromised, the relationship between the victims of the breach and the data custodian (including any relevant contractual relationship or state laws governing the relationship), and what is known about the source of the breach, if anything. Ultimately, if courts continue to come to differing outcomes in factually analogous cases, the Supreme Court may choose to address the split and have the final word on the issue.