AN A.S. PRATT PUBLICATION
NOVEMBER/DECEMBER 2018
VOL. 4 • NO. 9

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis®

Pratt's Privacy & Cybersecurity Law Report

VOLUME 4 | NUMBER 9 | NOVEMBER-DECEMBER 2018

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*, [4] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [281] (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

(2018–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, 646.539.8300. 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.

Fourth and Eighth Circuits Address Injury in Data Breach Cases

By Roger A. Cooper and Miranda Gonzalez*

Two federal circuit courts of appeals recently grappled with injury requirements in the data breach context. The authors of this article discuss the decisions.

The nature of any injury suffered by individuals from a cyber incident continues to be a major issue in data breach litigation. The U.S. Supreme Court has thus far declined to address the issue of Article III standing in the data breach context, resulting in an ongoing circuit split on whether data theft is by itself sufficient to satisfy Article III's injury requirements.[1] Two federal Circuit Courts of Appeals recently grappled with injury requirements in the data breach context.

THE FOURTH CIRCUIT'S DECISION IN *NBEO*

On June 12, 2018, the U.S. Court of Appeals for the Fourth Circuit vacated a district court's dismissal and held that plaintiffs possessed Article III standing because they suffered actual harm when credit card accounts were opened using their personal information.[2] In that case, a putative class of optometrists sued the National Board of Examiners in Optometry, Inc. ("NBEO") for its failure to adequately safeguard their personal information after the NBEO suffered a data breach. The district court had dismissed the complaints based on lack of Article III standing, but the Fourth Circuit vacated the judgment, finding plaintiffs had adequately plead injury-in-fact that was sufficiently traceable to the NBEO.

Specifically, the Fourth Circuit held that while a "mere compromise of personal information, without more, fails to satisfy the injury-in-fact element," plaintiffs had sufficiently alleged actual harm because their data had been accessed and used to open credit card accounts without their knowledge or approval. In addition, plaintiffs incurred out-of-pocket costs when purchasing credit monitoring services and lost the value of their time in seeking to notify credit reporting agencies and the Internal Revenue Service of the data breach. The Fourth Circuit observed that, although costs for mitigating measures to safeguard against future identity theft do not normally

* Roger A. Cooper is a partner at Cleary Gottlieb Steen & Hamilton LLP focusing his practice on complex civil litigation, with an emphasis on disputes arising out of securities, mergers and acquisitions, and derivative transactions, as well as on corporate governance issues. Miranda Gonzalez is a litigation associate at the firm. The authors may be contacted at racooper@cgsh.com and mirgonzalez@cgsh.com, respectively.

[1] *See 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); *In re SuperValu, Inc.*, 870 F.3d 763 (8th Cir. 2017).

[2] *Hutton v. Nat'l Bd. of Exam'rs in Optometry, Inc.*, 892 F.3d 613 (4th Cir. 2018).

constitute injury-in-fact, the Supreme Court has recognized an injury from such costs when a substantial risk of harm actually exists.[3] The Fourth Circuit further held that the injury was traceable to NBEO because amongst the group of optometrists, NBEO was the only common source that collected and continued to store social security numbers that were required to open credit card accounts and it had also stored outdated personal information during the relevant time periods.

THE EIGHTH CIRCUIT'S DECISION IN *TARGET*

On June 13, 2018, the U.S. Court of Appeals for the Eighth Circuit affirmed certification of a settlement class in the Target data breach litigation, finding that there was no intraclass conflict between class members who suffered verifiable losses from the breach and those who did not.[4] The district court had certified a class for settlement purposes of persons whose credit or debit card information and/or whose personal information was compromised as a result of the data breach that was first disclosed by Target on December 19, 2013. Under the agreement, Target agreed to pay $10 million to settle the claims of all class members. For class members with documented proof of loss, the agreement called for full compensation of their actual losses up to $10,000 per claimant. For class members with undocumented losses (i.e., who did not submit claims for reimbursement), the agreement directed a pro rata distribution of the amounts remaining after payments to documented-loss claimants. In addition, Target agreed to implement a number of data-security measures and to pay all class notice and administrative expenses. Two class members objected to the settlement, relying on the Supreme Court's decisions in *Ortiz* and *Amchem* to argue that there was an intraclass conflict between class members who suffered verifiable losses from the data breach and those who did not, and that each subgroup necessitated separate legal counsel.[5]

The Eighth Circuit rejected the objection and affirmed certification of the settlement class, holding that that there was no fundamental conflict requiring separate representation. The court held that, unlike *Ortiz* and *Amchem* where the asbestos-related injuries were extraordinarily various, here all class members suffered the same injury, i.e., compromise of their personal and financial information from the data breach. Class representatives included plaintiffs who submitted claims for monetary damages and identified losses incurred in the data breach and plaintiffs who did not submit such claims but faced future risk of harm. Moreover, both groups faced the same possibility of unknown future harm; for example, it was equally likely that a line of credit would be opened using personal information from a class member with documented losses as it would from a class member with no documented losses.

[3] *See Clapper v. Amnesty Int'l USA*, 568 U.S. 398 (2013).
[4] *In re Target Corp. Customer Data Sec. Breach Litig.*, 892 F.3d 968 (8th Cir. 2018).
[5] *See Ortiz v. Fibreboard Corp.*, 527 U.S. 815 (1999); *Amchem v. Windsor*, 521 U.S. 591 (1997).

The court also emphasized that the value of the injunctive relief was offered to both groups under the settlement so that no class member released claims without consideration.

CONCLUSION

The recent decisions by the Fourth and Eighth Circuits were in line with prior precedent in the data breach context, given that at least some, if not all, plaintiffs in both cases suffered verifiable losses that were more than mere allegations of data theft. However, the cases highlight the fact that the injury suffered by individuals following data breach – or lack thereof – continues to be perhaps the most prominent issue in such litigation. This makes it all the more important that companies that suffer cyber incidents consider the steps that they can take to investigate (in a privileged manner) whether any injury has occurred and appropriately document any findings, including in anticipation of any resulting litigation.