AN A.S. PRATT PUBLICATION
MAY 2022
VOL. 8 NO. 4

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 8 **NUMBER 4** **May 2022**

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*, [8] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [113] (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

(2022–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, 631.291.5541. 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 Litigation Review and Update

By Nancy R. Thomas and Matt Wyatt*

This article describes recent cyber incident highlights and discusses what we can expect the rest of this year.

Cyber incidents top the list of issues keeping in-house counsel up at night. And as we continue to see the number of incidents climb, we continue to see class actions filed in their wake. This article describes recent cyber incident highlights and discusses what we can expect the rest of this year.

CLASS ACTION FILING TRENDS

We counted 36 major data breach class actions filed last year, treating multiple cases filed against a single defendant as one major class action.[1] This is a significant increase over the 25 major class actions filed the prior year. Here's what we are seeing in these cases:

Plaintiff's Counsel Continue to Jockey for Position

Plaintiff's attorneys continue to try to beat others to the courthouse. In five of the major data breach cases filed, plaintiffs filed the first-filed case within a week of announcement of the breach. On average, cases were filed within four weeks of the announcement. Three of the cases were the subject of multidistrict litigation ("MDL") proceedings; 21 of them were consolidated.

What Was Stolen?

In 26 cases, plaintiffs alleged exfiltration of social security numbers, significantly more than the number of cases in 2020. Last year, the majority of cases concerned allegedly compromised payment card information. This kind of information allegedly was compromised in about one-third of the cases in 2021, and about half of the cases concerned alleged exfiltration of sensitive medical data.

---

* Nancy R. Thomas, a partner at Morrison & Foerster LLP, is a consumer class action and regulatory enforcement lawyer who represents clients in a broad range of complex matters, including financial services, privacy and data security and wage and hour matters. She may be reached at nthomas@mofo.com. Matt Wyatt, an associate in the firm's Litigation Department, may be reached at mwyatt@mofo.com.

[1] In gathering these cases, we defined major data breach litigation as cases in which multiple actions were filed regarding the same incident.

Who Was Impacted?

As compared to 15 percent of the cases in 2020, plaintiffs in about one-third of the cases in 2021 were employees. The rest of the plaintiffs were customers, patients or account holders.

Novel Liability Theories

We saw further evolution of plaintiff's counsel's theories in 2021. In a suit filed in response to the Colonial Pipeline ransomware attack, for example, plaintiff alleges that consumers and gas station owners were harmed by increased gas prices as a result of the company's negligence.[2] And a federal court in Los Angeles followed other courts in rejecting plaintiff's theory that the value of his personal information decreased due to the breach.[3]

RULINGS ON MOTIONS TO COMPEL ARBITRATION AND FOR CLASS CERTIFICATION

Motions to Compel Arbitration

Defendants in several of these cases had filed motions to compel arbitration. We have seen several rulings on these motions, including five in which courts enforced a class action waiver and ordered plaintiffs to arbitrate their claims on an individual basis. We did not see any data breach-specific arguments made by plaintiffs in opposing these motions.

Class Certification

Courts issued two decisions on motions to certify a class in data breach cases in 2021. The courts reached opposite conclusions on whether plaintiffs met their burden to show common issues predominate over individual issues, particularly as to questions of causation and damages.[4] The courts reached different conclusions on two key issues: (a) whether plaintiffs could prove that the data breach caused them harm on a class-wide basis, including in particular how exfiltration of plaintiff's and putative class members'

---

[2] *See* Class Action Complaint, *Dickerson v. CDPQ Colonial Partners, L.P.*, No. 1:21-cv-02098 (N.D. Ga. May 18, 2021).

[3] *Rahman v. Marriott Int'l, Inc.*, No. SA CV 20-00654-DOC-KES, 2021 U.S. Dist. LEXIS 15155 (C.D. Cal. Jan. 12, 2021).

[4] *McGlenn v. Driveline Retail Merch., Inc.*, No. 18-cv-2097, 2021 U.S. Dist. LEXIS 9532 (C.D. Ill. Jan. 19, 2021) and *In re Brinker Data Incident Litig.*, No. 3:18-cv-686-TJC-MCR, 2021 U.S. Dist. LEXIS 71965 (M.D. Fla. Apr. 14, 2021).

data in other breaches impacted the analysis, and (b) whether expert testimony can get plaintiffs over the hurdle of individualized issues regarding whether the data breach caused a putative class member any harm. The U.S. Court of Appeals for the Eleventh Circuit granted a Rule 23(f) petition to consider the trial court's ruling granting class certification, so watch for further developments here.

THE PRIVILEGE WARS CONTINUE

We continue to see courts compel disclosure of reports prepared by incident response consultants hired by counsel. In two decisions, the courts basically followed the analysis of the *Capital One* rulings in 2020.[5] Both courts focused on whether the report served a broader purpose than assisting in preparation for litigation. The courts viewed distribution of the report beyond the legal team, whether within the company or to law enforcement as evidence that the work would have been conducted regardless of the lawsuit. One of the courts looked to the purpose stated in the SOW in finding the report contained facts, not attorney-client privileged information. These decisions add to the growing number of courts expressing skepticism about claims of attorney-client privilege or work product protection for incident response reports.

SETTLEMENT TRENDS

We count 16 settlements in major federal data breach cases in 2021. A few takeaways:

Claims-Made Settlements Made a Comeback

We continue to see data breach settlements follow one of two well-developed templates: injunctive relief and offer of credited monitoring services combined with either a claims-made settlement (sometimes with an aggregate cap) or a settlement fund. As compared to 2020, we see an increase in the number of claims-made settlements (nine in 2021, compared to four in 2020) and a reduction in settlement funds (six in 2021, compared to nine in 2020).

We also saw one settlement under Rule 23(b)(2). Defendant agreed to injunctive relief, but there was no individual relief for settlement class members.

[5] *Wengui v. Clark Hill, PLC*, 338 F.R.D. 7 (D.D.C. 2021); *In re Rutter's Data Sec. Breach Litig.*, No. 1:20-CV-382, 2021 U.S. Dist. LEXIS 136220 (M.D. Pa. July 22, 2021).

Very Low Claims Rates

Claims rates for monetary relief in claims-made settlements were very small, between 0.1 percent and one percent of settlement class members. The rate of enrollment in credit monitoring products ranged from 0.8 percent to 5.2 percent in the two cases in which it was reported in the papers supporting final approval. Plaintiffs submitted information about the total amount of monetary relief in only a couple of the cases. For those cases, plaintiffs reported total monetary relief of roughly $840,000 (compared to $1,575,000 awarded for attorney's fees and costs) and $300,000 (compared to $739,000 awarded for attorney's fees and costs).

Longer Litigation, Higher Fees

No surprises here. The longer the litigation, the higher the legal fees. Courts awarded an average of $270,000 for cases pending up to 18 months as compared to an average of $1.3 million for cases pending more than 18 months (excluding one outlier settlement with attorney's fees nearly twice the next highest fees amount).

Few Objectors

There were no objections filed in 11 of the 16 cases. In the rest of the cases, the number of objectors was small, less than .002 percent of settlement class members. An appeal was filed in only one case.

WHAT TO WATCH FOR

Even with the significant increase in major data breach litigation filed in 2021, we again predict that we will see even more major data breach cases filed this year given the enormous increase in all types of security incidents in 2021. It will be important to watch the briefing and the Eleventh Circuit's ruling on the district court's order granting class certification in the *Brinker* data breach litigation. The appeal tees up several related issues we see in all data breach class actions, including whether the court can certify a class in which the majority of putative class members have no injury and therefore lack Article III standing, whether individual issues predominate in proving harm caused by the breach, and whether plaintiffs can rely on an expert opinion attempting to smooth out individual issues by proposing an average amount of damages per putative class member.