AN A.S. PRATT PUBLICATION
MAY 2024
VOL. 10 NO. 4

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 10 **NUMBER 4** **May 2024**

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
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home
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) 487-3385

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*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [179] (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

(2024–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.

Current Issues In Data Breach Class Action Settlements

By Mark A. Olthoff and Shundra Crumpton Manning*

In this article, the authors discuss a number of recent developments impacting the settlement of data breach class actions.

Very few civil cases ever reach a jury. Nearly every lawsuit is at some point resolved by the court on motion or through settlement. Class action cases are no different, including those filed after data breach incidents.

Accordingly, developing a strategy early in a lawsuit timeline is critical – whether to seek an early dismissal or an early out of court resolution. This article discusses a number of recent developments impacting class action settlements. Whether a case settles for tens of millions of dollars or substantially less, these recent events should be a part of any settlement consideration.

CLASS CERTIFICATION

First, two federal courts recently certified classes in data breach cases. Both cases were appealed and, in each instance, the appeals courts reversed or vacated the district court decisions (albeit for different reasons). While the lower courts' certification orders demonstrate data breach cases can be appropriate for class treatment, the fact that appeals courts have closely scrutinized the district courts' conclusions also shows there is uncertainty. In turn, a well-known axiom for any settle environment is where uncertainty exists on either or both sides.

CLAIMS RATES AND NOTICES

Second, courts, particularly in the federal system, are increasingly scrutinizing settlements in terms of fairness, reasonableness, and result. Courts are evaluating the claim rates and adequacy of notices being used. A California federal judge recently complained that predicted rates of 1%-9% were too low. He also found that the settlement notice provided to class members was too long and complicated. In denying the plaintiffs' motion for preliminary approval, the judge told the lawyers to find a way to boost up the expected number of claims.

In another recent instance, a Michigan federal judge became irked when the settlement presented to him describing potential payouts failed to consider that settlement costs

* The authors, attorneys with Polsinelli PC, may be contacted at molthoff@polsinelli.com and scmanning@polsinelli.com, respectively.

and attorney fees were being deducted from the settlement fund. He found the notice was misleading and rejected preliminary approval.

The U.S. Court of Appeals for the First Circuit also recently vacated a class settlement where it found significant differences in the claims created conflicts within the class requiring separate class representatives and would not allow for equal treatment of class awards.

Finally, the U.S. Court of Appeals for the Second Circuit vacated a settlement finding there is no "presumption of fairness" as to a settlement agreement that was negotiated at arm's length during a lengthy mediation before a neutral party. Rather, district courts must fully analyze all aspects of a settlement under the factors in Rule 23.

AGGREGATORS AND ARTIFICIAL INTELLIGENCE

Relatedly, another somewhat recent development is the introduction of third-party aggregators using artificial intelligence (AI) to boost objection, opt-out, and claims rates. In essence, aggregators are using AI to locate class members and then communicate with them to file objections, opt-outs (with the possibility of filing other suits), or submit claims on behalf of the class members. At least one court has sounded an alarm and rejected the use of an AI aggregator for these purposes.[1] The court overruled objections and set aside aggregated claims reasoning there was a lack of control over class communications and notice.

On the other hand, some commentators have expressed that the use of AI could lead to more class member participation, better class notice, improvements in class administration, and higher claim rates. That said, AI is not a panacea for all problems and safeguards to prevent abuses and fraud would have to be implemented.

ATTORNEYS' FEES

Counsel fees continue to be a source of judicial consternation and a number of courts have continued to question attorneys' fee awards in settlements. In a June 2023 opinion by the U.S. Court of Appeals for the Ninth Circuit, the court reversed (and revoked) a district court order where the plaintiffs initially sought $6 million and the court reduced it to $1.7 million.

Still, the appeals court rejected the amount because – in the claims-made settlement – only $53,000 in compensation was claimed. This resulted in attorneys' fees of more than 30 times the amount. This case and others like it are now being used to change class action settlement structures. Plaintiffs are aggressively pushing for settlement terms that include non-monetary class-wide relief such as credit monitoring or certain forms of injunctive relief to demonstrate the value of the class settlement. There are also a

[1] See In re Juul Labs, Inc. Marketing, Sales Practices, and Products Liability Litigation (N.D. Cal. Sept. 19, 2023).

significant number of cases where plaintiffs are demanding a common fund structure (as opposed to claims-made) to reduce the risk that settlements are not approved because they do not sufficiently compensate class members.

Historically, claims-made settlements have been a better approach in data breach settlements because the structure permits compensation to be awarded to those class members that have interest in the settlement and have been harmed by the incident. A common fund structure, on the other hand, merely distributes a settlement fund without regard to anyone's possible damage – potentially resulting in overpayments and underpayments to particular class members.

RESIDUAL SETTLEMENT FUNDS

Finally, residual settlement funds have received attention in the past year. Frequently, in a common fund settlement, these are funds remaining due to an inability to locate every class member. Several alternatives exist to distribute the remainder:

(1) Reversion to the defendant;

(2) Re-distribute to the class members who are known;

(3) Distribute to a cy pres recipient; or

(4) Escheat to a government.

Ordinarily, courts reject returning money to the defendant that paid to settle and, in some instances, it is infeasible or uneconomical to re-distribute to the class members. This leaves alternatives (3) or (4) most likely. In the past year, courts have continued to struggle with the tension of distributing money to a cy pres recipient that has no connection to the lawsuit and judges determining how much should be awarded to any particular organization. In addition, critics have commented that cy pres awards divert funds from the real beneficiaries of the settlement. This said, courts have recently approved both cy pres distributions and awarded residual funds to the U.S. Treasury.

The validity and application of cy pres and other alternatives will continue to be addressed by the courts.

CONCLUSION

Each of these developments will continue to impact the future of data breach class actions and settlements. There are opportunities to be creative and seek novel ways to resolve these claims and parties and counsel alike should be open to building settlements that can reach the proposed classes yet also consider the necessary safeguards to protect against abuses.