AN A.S. PRATT PUBLICATION
JUNE 2021
VOL. 7 • NO. 5

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 7 **NUMBER 5** **June 2021**

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*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [143] (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

(2021–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.

Data Breach's Lack of "Sensitive Information" Creates Barrier to Standing in Federal CCPA Lawsuit

By Spencer Persson*

The U.S. District Court for the Central District of California recently answered the question of whether challenges to standing of California Consumer Privacy Act data breach claims brought in federal court could still be effective, when it granted defendant's motion to dismiss in Rahman v. Marriott. *The author of this article discusses the decision.*

More than a year after the California Consumer Privacy Act ("CCPA") became operative, the proverbial jury was still out on whether challenges to standing of CCPA data breach claims brought in federal court could still be effective. The U.S. District Court for the Central District of California seemingly answered that question in the affirmative when it granted defendant's motion to dismiss in *Rahman v. Marriott*.[1]

BACKGROUND

In *Marriott*, the plaintiffs alleged six causes of action against the defendant: negligence, violation of the CCPA, breach of contract, breach of implied contract, unjust enrichment, and violation of California's Unfair Competition Law. The incident in question occurred when two Marriott franchise employees in Russia accessed class members' name, address, phone number, email address, gender, birth date, and loyalty account number information.

The district court held that it lacked subject matter jurisdiction over plaintiffs' claims due to plaintiffs' inability to establish Article III standing. The court ruled that plaintiffs could not establish the "injury-in-fact" required for standing because the type of information accessed did not include "*sensitive* information, such as social security numbers, credit card information, or passwords."

Absent such sensitive information, the court found that there was no credible risk of identity theft or financial loss. The court also rejected plaintiffs' theory that the value of their information had been diminished in some manner or that plaintiffs should be compensated for mitigation costs. Regarding the latter argument, the court took the

* Spencer Persson, CIPP/US, a partner at Davis Wright Tremaine LLP, is an experienced litigator with the firm's privacy, security, and technology group, where he represents clients in data privacy matters and consumer class actions. He may be reached at spencerpersson@dwt.com.

[1] Case No. 20-cv-00654, Dkt. 34 (C.D. Cal. April 3, 2020).

position that "'mitigation costs . . . rise and fall together' with claims based on the risk of future harm."

COURT STEERS CLEAR OF APPLYING BIPA ARGUMENT TO ESTABLISH STANDING

Surprisingly, the court did not address plaintiffs' argument, relying on *Patel v. Facebook, Inc.*,[2] that unauthorized access itself is a tangible injury giving rise to standing.

In *Patel*, the U.S. Court of Appeals for the Ninth Circuit held that the Illinois Biometric Information Privacy Act ("BIPA") created a privacy right in Illinois residents' biometric information that – when obtained without authorization – gives rise to a statutory injury sufficient to confer Article III standing.

In their opposition, plaintiffs attempted to apply this holding generally to all of their claims. Had they limited this argument to their CCPA claim, the court may have addressed it specifically and decided whether, like BIPA, the CCPA creates a statutory right of privacy in personal information obtained through an unauthorized data intrusion such that the mere access and exfiltration of such information creates an injury sufficient to confer standing.

In this instance, though, it probably would not have made any difference because the court could have also dismissed the CCPA claim under Rule 12(b)(6) (failure to state a claim) rather than Rule 12(b)(1) (lack of jurisdiction). Specifically, the court could readily have adopted Marriott's argument that the exposed information on its face did not qualify as "personal information" under Cal. Civ. Code § 1798.81.5(d)(1)(A), incorporated by reference into the CCPA's private right of action provision at Section 1798.150(a)(1).

Because the court dismissed the matter for lack of standing, it did not reach this argument. Nor did the court address whether plaintiffs could seek statutory damages under the CCPA where (as appears to be the case here) they failed to fulfill the 30-day pre-suit notice requirement under Section 1798.150(b). Ultimately, whether a well-pled CCPA claim in federal court remains subject to an Article III challenge remains an open question, as does whether plaintiffs' claims might have proceeded into discovery in state court, where standing is not typically required.

DO CCPA CLAIMS INCREASE DATA BREACH SETTLEMENTS?

Whether CCPA claims increase the settlement value of cases also remains an open question. For example, the U.S. District Court for the Northern District of California

[2] 932 F.3d 1264, 1271 (9th Cir. 2019).

granted preliminary approval of the *Hanna Andersson* settlement, the terms of which are similar to those settlements reached prior to passage of the CCPA.

On December 11, 2020, another classwide settlement received preliminary approval in *Llamas v. Truefire*,[3] pending in the U.S. District Court for the Middle District of Florida. *Truefire* is a purveyor of online guitar lessons and suffered a credit card breach from August 3, 2019, to January 14, 2020. The named plaintiff, located in California, allegedly incurred fraudulent charges on their card. Plaintiff asserted a CCPA claim but did not seek statutory damages, likely reflecting that he did not provide the requisite 30-day notice by letter prior to filing the complaint.

The *Truefire* settlement includes nine months of complimentary access to Truefire, reimbursements of up to $60 for time spent remediating payment card issues, $50 per California sub-class member for damages under the CCPA, and Truefire's agreement to implement certain security and privacy improvements. Plaintiffs estimated the settlement value as exceeding $1.2 million, with almost $900,000 of that value tied to complimentary access for the 4,911 class members.

There were 733 California class members eligible for the $50 payment, meaning that less than $40,000 of the possible settlement value can be directly tied to the CCPA. Truefire has agreed not to oppose a fee and cost application of up to $156,500.

Finally, this is a "claims made" settlement, so Truefire's actual out-of-pocket settlement costs are unlikely to approach the $1.2 million figure. Like the *Hanna Andersson* settlement, *Truefire* did not appreciably move the goalposts for classwide data breach claims despite including a CCPA claim.

Several more decisions involving CCPA claims are likely to be issued over the next 60 days, including motions to dismiss and a motion to compel arbitration (and enforce a class action waiver). Until then, we will have to be content with what little we have gleaned from the sparse number of CCPA data breach cases that have been brought to fruition.

[3] Case No. 20-cv-00857.