AN A.S. PRATT PUBLICATION
APRIL 2018
VOL. 4 • NO. 3

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 4 | NUMBER 3 | APRIL 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 [73] (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, 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.

Incident Response – Privilege and Work Product Issues After *In re Premera*

By Molly McGinnis Stine and Brandan Montminy*

Very few opinions have addressed the application of attorney-client privilege and the work-product doctrine to the materials created by such work. Recently, in In re Premera Blue Cross Customer Data Sec. Breach Litig.*, the U. S. District Court for the District of Oregon provided detailed analysis of the issues. The authors of this article discuss the decision and suggest some steps that an entity may want to consider to try to protect the work concerning its incident response.*

Despite considerable incident response work after numerous alleged data breaches, very few opinions have addressed the application of attorney-client privilege and the work-product doctrine to the materials created by such work.

IN RE PREMERA

Recently, in *In re Premera Blue Cross Customer Data Sec. Breach Litig.*,[1] the U. S. District Court for the District of Oregon provided detailed analysis of the issues. The opinion concerned a class action brought against Premera after Premera's March 17, 2015 disclosure that its computer network had been breached. The plaintiffs alleged that the breach compromised the confidential information of approximately 11 million current and former members, affiliated members, and employees of Premera. The plaintiffs requested an order to compel Premera to produce certain documents, described by category, that Premera had withheld on assertions of attorney-client privilege or the work-product doctrine.

Materials Sought

The four categories of materials sought by plaintiffs' counsel were:

(1) documents that Premera asserted incorporated the advice of counsel, but which were not prepared by or sent to counsel;
(2) documents that Premera asserted were prepared at the request of counsel, but were not prepared by or sent to counsel and appear to be business documents not prepared because of litigation;

* Molly McGinnis Stine is a partner at Locke Lord LLP, and a member of the firm's Insurance: Litigation and Counseling practice group, the Steering Committee of the firm's Privacy & Cybersecurity practice group, its Incident Response Team, and its New York Department of Financial Services initiative. Brandan Montminy is an associate at the firm focusing his practice on a variety of matters arising from banking and finance, commercial, construction, insurance, and product liability disputes. The authors may be contacted at mmstine@lockelord.com and brandan.montminy@lockelord.com, respectively.

[1] D. Or., Oct. 27, 2017.

(3) documents that relate to third-party vendor work on the data breach investigation and remediation; and
(4) documents that Premera sent to third-parties Premera asserts are subject to the joint defense or common interest exception to the waiver of privilege by disclosure.

Although all four categories and the court's discussion of each are relevant and should be reviewed, this article focuses on the third category – the documents relating to the work done by Mandiant, a third-party cybersecurity firm.

The court began by referring to the general law of attorney-client privilege and work-product doctrine applicable to all privilege disputes. Importantly, the court continued the reasoning of the U. S. District Court, C.D. California, in applying the "because of" test to potential work-product materials prepared for dual purposes – litigation and any other – in the context of materials prepared following a data breach.

The third category of documents is of particular interest because it addresses, among others, documents relating to Mandiant's work for Premera. Mandiant was hired by Premera in October 2014 to review Premera's data management system. On January 29, 2015, Mandiant discovered the existence of malware in Premera's system. On February 20, 2015, Premera hired outside counsel in anticipation of litigation as a result of the breach. The next day, on February 21, 2015, Premera and Mandiant entered into an amended statement of work that shifted supervision of Mandiant's work to outside counsel. However, the amended statement of work did not otherwise change the scope of Mandiant's work from what was described in the Master Services Agreement between Mandiant and Premera entered into on October 10, 2014.

In re Target Corp. Customer Data Sec. Breach Litig.

The court found that the amended statement of work did not support that Mandiant's focus shifted to an investigator working on behalf of outside counsel, and that the materials were not protected. In reaching its conclusion, the court differentiated two of the few relevant, prior cases. The first was *In re Target Corp. Customer Data Sec. Breach Litig*.[2] In that case, Target had dual-tracked the investigation and engaged separate teams: one to investigate the data breach generally, and the other to investigate through a company retained by counsel for the purpose of assisting the attorneys in providing legal advice and preparing for litigation. The *Premera* court described the distinction between the circumstances before it and those in *Target:*

> With Premera, however, there was only one investigation, performed by Mandiant, which began at Premera's request. When the supervisory responsibility later shifted to outside counsel, the scope of the work performed did not change. Thus, the change of supervision, by itself, is not sufficient to render all of the later communications and underlying documents privileged or immune from discovery as work product.

[2] D. Minn., Oct. 23, 2015.

In re Experian Data Breach Litigation

Similarly, the court distinguished *In re Experian Data Breach Litigation*.[3] In *Experian*, outside counsel was hired by the company and outside counsel then hired Mandiant. However, here, Premera had already hired Mandiant, which was performing an ongoing investigation under Premera's supervision before outside counsel became involved. The Premera court made it clear that Premera had the burden of showing that Mandiant changed the nature of its investigation, and failed to meet that burden.

This failure to sufficiently amend the statement of work was ultimately fatal to both assertions of attorney-client privilege as well as work-product protection. The *Premera* court did allow that Premera could properly withhold materials that were not "dual purpose," were prepared "for the purpose of communicating with an attorney" for legal advice, or did contain "the mental impressions of counsel prepared in anticipation of litigation."

CONCLUSION

This new decision and those before it collectively suggest some steps that an entity may want to consider to try to protect the work concerning its incident response. Each matter is different and the facts and applicable law of any given situation may affect whether attorney-client privilege and work product protection apply. While any entity should evaluate its own situation and consider discussing these issues with counsel, the following are among the possible topics about which to assess timing and relative merits:

- identify and engage incident response counsel as soon as possible, working with one's insurer depending on the type of insurance coverage that may be involved;
- have incident response counsel retain and direct the work of other third-party service providers;
- have engagement letters appropriately indicate what work is being requested and for what purpose, including its role in assisting counsel in providing legal advice and in anticipation of litigation;
- consider two parallel investigations as in *Target*; and
- develop a strategy about with whom, internally and externally, incident response work is discussed and shared.

[3] C.D. Cal., May 18, 2017.