



DATA BREACH RULING POTENTIALLY NARROWS SCOPE OF PRIVILEGE AND WORK-PRODUCT ASSERTIONS

By Kelso L. Anderson, *Litigation News* Associate Editor

A discovery order issued by a federal district court both compelled and restricted the production of documents in a data breach case. The ruling has elicited conflicting views from ABA Section of Litigation leaders as to whether it narrowed the attorney-client privilege and work-product immunity doctrine. Despite their conflicting views, Section of Litigation leaders agree that the ruling sends a clear signal to businesses: Develop plans now that protect documents and communication against discovery for any potential data breach.

GENESIS OF DATA BREACH AND SCOPE OF DISCOVERY REQUEST

In *In re Premera Blue Cross Customer Data Security Breach Litigation*, the plaintiffs brought a class action lawsuit

against the defendant, a health care benefits service provider, after the defendant publicly disclosed in 2015 that its computer network was breached, resulting in the disclosure of personal and confidential information of the plaintiffs—more than 10 million current and former members and employees of the defendant. The plaintiffs alleged that the breach began in 2014 and that the defendant unreasonably delayed notifying the affected parties until 2015.

As part of their lawsuit, the plaintiffs moved to compel production of four categories of documents: (1) documents the defendant asserted include advice of counsel but were not sent to or prepared by counsel; (2) documents the defendant 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; (3) documents that relate to third-party vendor work on data breach investigation and remediation, including documents related to technical and public relations aspects of the vendor investigation and analysis; and (4) documents that the defendant sent to third parties but asserted were part of a joint defense or common interest exception to waiver or privilege.

APPLICATION OF DISCOVERY PROTECTIONS TO DOCUMENT CATEGORIES

In considering the plaintiff's motion to compel production of the foregoing categories of documents, the U.S. District Court for the District of Oregon set forth the general rules on attorney-client privilege and work-product doctrine. Among other things, the district court noted that the attorney-client privilege is governed by state law and "protects only communications and advice between attorney and client." Further, the court observed that the privilege does not "shield facts from discovery." Embracing the "flexible approach" to the privilege announced by the U.S. Supreme Court in *Upjohn Co. v. United States*, the court further stated that nonmanagerial employees may qualify as "clients" for purposes of asserting the privilege.

As to the work-product doctrine, the court explained that federal law protects the doctrine and "is not a privilege but a qualified immunity protecting from discovery documents and tangible things prepared by a party or his representative in anticipation of litigation." Additionally, the court observed that the doctrine protects core work product—an attorney's mental impressions and opinions—and a party may only obtain such work product upon a showing of "compelling" need. Finally, the court noted that the "common interest doctrine" is governed by state law and generally applies where multiple parties share confidential communication relating to common claims or defenses. The common interest doctrine is an exception to the general rule that a "voluntary disclosure of privileged attorney-client privilege or work product communication to a third party waives the privilege," the court stated.

Applying these legal principles, the court concluded that many of the documents in category 1—documents prepared by the defendant's employees that incorporated advice of counsel but were not sent to counsel—were not privileged because they were business documents that the defendant would have prepared without regard to litigation. However, the court concluded that drafts or edits to business documents that incorporated defense counsel's views were protected. Similarly, the court found that, except when counsel expressly rendered legal advice, many category 2 documents—documents the defendant alleges its employees prepared at counsel's request—were not privileged because they included press releases and other

public-relations documents to perform a business function.

As to category 3 documents—third-party reports commissioned by the defendant in response to the data breach—the court concluded those documents were not protected by the work-product doctrine because they were not prepared in anticipation of litigation. In so concluding, the court distinguished *In re Target Corp. Customer Data Security Breach Litigation* and *In re Experian Data Breach Litigation*, cited by the defendant for the proposition that its counsel supervised the third party's data breach investigation and remediation and, therefore, the report was protected work product. According to the court, the scope of the work performed

"Having a response plan in place reduces the likelihood of a misstep that could result in waiver of the attorney-client privilege and work-product protections."

by the third party did not change; what changed was the supervision of the third party—from defendant to defendant's counsel—which was an insufficient basis to warrant the work-product protection.

The court concluded that the defendant's common interest exception asserted under category 4 documents—documents shared with third parties but withheld by the defendant based on an assertion of the exception—was inapplicable because the alleged third parties with whom

documents were shared were not subject to the *present* data breach but, instead, were the subject of *past* data breaches. On this point, despite finding no "common interest" to protect from discovery documents sent to third parties, the court concluded that the defendant believed in "good faith" that those documents would be subject to the exception. Accordingly, the court allowed discovery of only oral communication, not documents, shared with third parties.

MIXED VIEWS

Section leaders had mixed views about the application of the attorney-client privilege and work-product doctrine to third-party vendors in this data breach case. "I thought the court did a good job balancing the need to protect attorney-client communications in the form of edits to various documents and seemed to err on the side of protection rather than disclosure," opined Robert J. Will, St. Louis, MO, cochair of the

Section's Pretrial Practice & Discovery Committee. "The lesson here is that clients and law firms should try their best to have third-party vendors compartmentalize their litigation-related and non-litigation-related work," Will concluded.

Other section leaders disagree with Will, believing the court "construed some privileges in an extremely narrow manner," says Kenneth M. Klemm, New Orleans, LA, also cochair of the Section's Pretrial Practice & Discovery Committee. For example, referring to Federal Rule of Civil Procedure 26(b)(3), third-party consultants "who will not testify generally remain outside the scope of discovery," adds Klemm. In data breach cases, "blanket claims of privilege are likely to fail," opines Barrett J. Vahle, Kansas City, MO, cochair of the Data Breach and Internet Subcommittee of the Section's Commercial & Business Litigation Committee. Instead, Vahle urges practitioners to have "specific objections" to discovery requests "in tandem with available procedural & evidentiary safeguards for the documents that are produced."

Disagreements aside, Section leaders agree that, in data breach cases, businesses should immediately consult counsel once a data breach is suspected. "Having a response plan in place reduces the likelihood of a misstep that could result in waiver of the attorney-client privilege and work-product protections," says Jeffrey D. Gardner, Phoenix, AZ, cochair of the Section's Trial Practice Committee. Likewise, "having in-house or, preferably, outside counsel involved from the very start usually renders a better result and, at the end of the day, allows protection from discovery of information developed for a lawyer to freely render legal advice," concludes Klemm. ❶

RESOURCES

- *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, No. 3:15-MD-2633-SI, 2017 U.S. Dist. LEXIS 178762 (D. Or. Oct. 27, 2017).
- *In re Target Corp. Customer Data Sec. Breach Litig.*, No. 14-2522 (PAM/JJK) (D. Minn. Dec. 18, 2014).
- *In re Experian Data Breach Litig.*, No. 8:15-cv-01592-AG-DFM (C.D. Cal. May 18, 2017).
- Fed. R. Civ. P. 26, available at <https://bit.ly/LN433-FRCP-26>.
- *Upjohn Co. v. United States*, 449 U.S. 383 (1981).