Cyber *Breach* Response:

Structuring the Investigation to Preserve Privilege

*By David Greenwald**

Cyber criminals continue to infiltrate data systems that house the personal, financial, and health information of millions of consumers. Financial institutions, credit rating agencies, health providers, and others have all been hacked.

In litigation filed in the wake of these data breaches, disputes frequently arise over whether documents generated by the targets of the cyber attacks are privileged, or must they be turned over in discovery. Plaintiffs seek to compel production of communications and work product prepared by third-party cyber consultants, and defendants assert attorney-client privilege and/or work product protections.

Since 2015, the courts have confronted this issue in a dozen cases.[1] In three of those matters, the court upheld assertions of privilege. In nine cases, the court compelled disclosure. While there are a number of factors that could explain the differences in outcomes, one reason may be the result of companies prioritizing the business imperative of remediating the data breach over taking sufficient steps to preserve privilege. The attorney-client privilege, which is owned by the company, is a corporate asset that a company may choose to impair in favor of urgent business needs. However, yielding privilege protection in a crisis – though practical under the circumstances – may not always be the result of careful consideration. This article explores factors that courts have considered in determining whether privilege should apply to safeguard materials from discovery and examines issues companies should consider before putting privilege protections at risk in breach litigation.

Continued on page 9

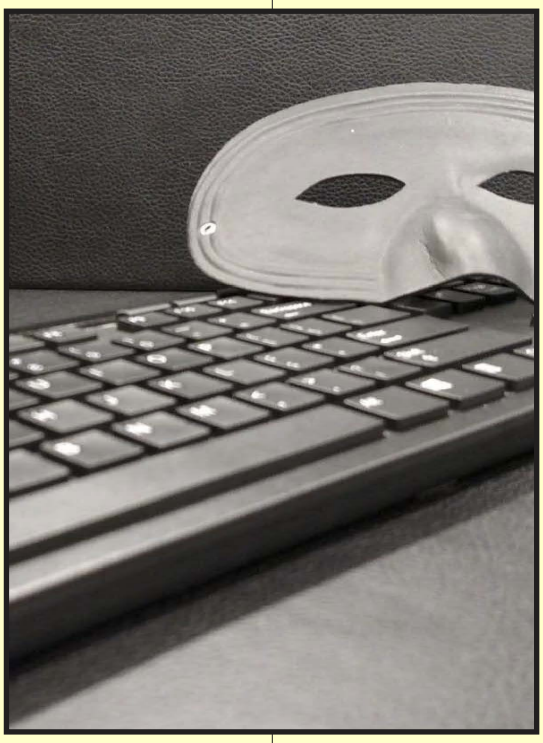
* *David M. Greenwald is a litigation partner with Jenner & Block LLP. Mr. Greenwald has tried cases in federal and state courts, arbitrated cases in the US and Europe, and conducted criminal and civil internal investigations on three continents. He is a co-author of* Testimonial Privileges *(West 2025), and co-editor of* Protecting Confidential Legal Information: A Handbook for Analyzing Issues Under the Attorney-Client Privilege and Work Product Doctrine, *(Jenner & Block 2023). Mr. Greenwald is a frequent speaker on topics relating to cross-border discovery, privilege, ethics, and e-discovery. He is a member of the firm's Aerospace and Defense practice.*

Cyber *Breach* Response

Continued from page 8

The Breach | Litigation | Privilege Scenario

Consider the typical scenario: A company discovers a data breach. The company immediately engages outside counsel, who then retains a third-party cyber consultant. The engagement letter includes the elements to establish the consultant as an agent of counsel within the company's attorney-client privilege: the consultant is being engaged to assist counsel to provide legal advice to the company; counsel will direct and supervise the consultant's work; the consultant will report directly to counsel; and the consultant agrees to take all reasonable steps to maintain applicable privileges and protections.



In subsequent litigation the question is whether the consultant satisfied the applicable standard to establish that the consultant was acting as an agent of counsel and, therefore, was within the company's privilege. Pursuant to what has come to be referred to as the "*Kovel* doctrine," a consulting expert retained by the attorney or the client to assist counsel to provide legal advice to the client qualifies as a privileged agent if consulted primarily for the purpose of analyzing complex information for counsel.[2]

When communications have dual legal and business purposes, a party must demonstrate that the primary purpose was legal (the majority approach),[3] or at least a significant purpose (the minority approach) of the communication.[4] As one court observed, the engagement letter may say that the consultant was engaged to assist counsel, but is that what the consultant actually did?[5]

Confronted with a massive data breach, a company has a business imperative: identify the cause of the breach; scope the damage; remediate the system; and implement corrective action to prevent future breaches. Taking an all-hands-on-deck approach, the company activates an internal incident response team that will be advised by third-party cyber consultants. Legal imperatives also confront the company, including providing legally sufficient notice to those whose data was hacked, in some cases choosing to notify the government pursuant to the Cybersecurity Information Sharing Act (CISA),[6] and preparing for anticipated litigation.

The courts have recognized the privilege where companies go to the extraordinary and possibly costly step of engaging two consultants – one to assist remediation efforts, and a second, walled off consultant to work with counsel.

Two-Track Investigations

In each of the three cases upholding privilege, the consultants engaged to assist counsel did not communicate their work to the company's incident response team. First, in *In re Target Corp. Customer Data Sec. Breach Litig.*,[7] the court held that the privilege and work product protections respectively applied to the consultant's communications and their work product prepared on behalf of counsel. The key factor was that the company established a two-track investigation, a non-privileged track conducted in the ordinary course of business, and a privileged track to educate counsel. Using the same consulting firm, in-house counsel engaged one team to work with the company's response team on remediation and corrective action. Outside counsel engaged a second team to work directly with counsel. The second team did not communicate with the response team.

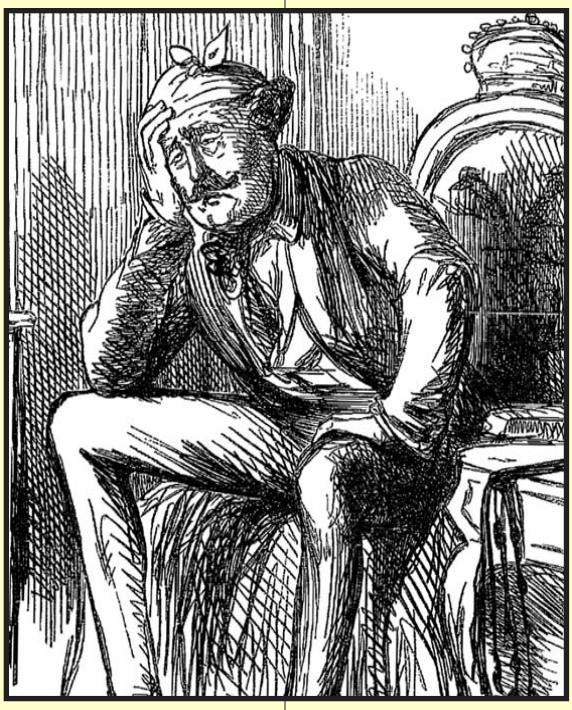
Next, the court in *In re Experian Data Breach Litig.,* upheld Experian's assertion of work product protections, noting that the court did not need to address the attorney-client privilege.[8] Immediately after discovering a breach, Experian engaged outside counsel, who straightaway engaged a cyber consultant. One day after Experian announced the data breach, the first complaint was filed. The complaint was then consolidated with over forty other consumer complaints. A few days after litigation was filed, the consultant provided a report to in-house and outside counsel, which they in fact used to develop their legal strategy. Disclosure of the report was very narrow and closely controlled by outside and in-house counsel. Significantly, the report was not given to Experian's incident response team or to the personnel working on remediation.

Continued on page 10

Cyber *Breach* Response

Continued from page 9

In their motion to compel, plaintiffs argued that work product protections should not apply to the report, because Experian had a duty to remedy, investigate and remediate the data breach. That is, Experian would have prepared the report even if litigation were not anticipated. The court rejected plaintiffs' argument, finding the report was prepared "because of litigation," that is, "but for" anticipated litigation, the report would not have been prepared in substantially the same form or with the same content.[9]



Lastly, the court in *Maldondo v. Solara Medical Supplies, LLC*[10] recognized both the attorney-client privilege and work product protections where Solara established a two-track investigation. The company walled off the consultant working with counsel from a second consultant who prepared a report for the sole purpose of responding to a Civil Investigative Demand (CID) issued by the FTC. In upholding privilege, the court noted that "one cannot imagine an attorney providing advice to a company faced with the complex litigation and regulatory issues resulting from a data breach, particularly where individuals' personal medical data is involved, without having a technical expert assist the attorney in investigating the facts."[11]

Target, Experian, and *Maldondo* all emphasize the importance of retaining two separate cyber consulting teams. Nevertheless, in the midst of a crisis, such a step may seem inconceivable and counterintuitive to corporate decision makers. First, establishing a two-track investigation undoubtedly adds significant cost that the company may consider unnecessary. Second, the business side of the company will press to obtain real-time information as the consultants conduct their investigations. The idea of engaging a cyber investigator who will not provide essential facts and insights to the remediation team in the midst of a crisis may seem in conflict with the best interests of the company. And yet, the cases are clear that doing so is likely the most effective way to preserve privilege or work product protection of the consultant's work.

Moreover, there are many examples of companies waiving privilege over investigative reports by acceding to the demands of senior business personnel that privileged reports be shared with employees who did not need access to legal advice. Doing so may lead a court to conclude that the report was prepared primarily for business purposes and is not privileged.[12]

Waiver could be avoided by having counsel draft a second, non-privileged document for business personnel that presents factual findings without disclosing the substance of privileged communications or the legal opinions of company counsel. Clients often push back against incurring additional time and attorneys' fees to prepare a non-privileged document when, in the view of business personnel, there is already a perfectly fine document that could be provided immediately. While cost control is important, disclosure of a privileged report to business personnel risks waiving privilege over the report and potentially additional privileged communications.

Factors Courts Found Defeated Privilege

In contrast to *Target, Experian,* and *Maldondo,* courts that have rejected privilege or work product claims have highlighted several factors that weighed against application of these immunities.

Lack of Two-Track Investigation: Several courts distinguished *Target* by noting that, unlike the two clear work streams that were walled off from each other in *Target,* the company had engaged only one consultant, which provided primarily business services.[13]

Delegation of Business Functions to Counsel: In several cases, the company engaged counsel to supervise a consultant to provide the same scope of work the consultant was already providing to the company as non-privileged business services. In *In re Premera,* defendant had engaged a consultant pursuant to a Master Services Agreement ("MSA") to review defendant's data management system a year before it discovered the data breach.[14] After the breach was discovered, defendant and the consultant entered into an amended statement of work that shifted supervision of the consultant's work to outside counsel. As the court observed, "[T]he only thing that changed was that [the consultant] was now directed to report to outside counsel and to label all of [the consultant's] communications as 'privileged,' 'work product,' or 'at the request of counsel.'" Delegating a business function to counsel, reasoned the court, does

Continued on page 11

Cyber *Breach* Response

Continued from page 10

not change the nature of otherwise unprotected communications and work product.[15]

Similarly, in *In re Capital One,* four years before a data breach, defendant entered into an MSA with a consultant to provide business services. Following the data breach, defendant engaged outside counsel, which entered into a Letter Agreement with the consultant whereby it would provide services and advice concerning "computer security incident response; digital forensics, log, and malware analysis; and incident remediation," *i.e.,* the same non-privileged services provided under the MSA.[16] Many courts have found that such a statement of work, articulated in various ways, constitutes business advice, not services intended to assist counsel.[17]

Broad Dissemination of Privileged Reports to Business Personnel: In several cases, companies disseminated otherwise privileged reports broadly to business personnel, thereby waiving privilege. For example, in *Capital One,* the consultant delivered its report directly to outside counsel, who sent it on to the company's legal department. Thereafter, the report was disseminated to 50 of defendant's employees, four regulators, and defendant's auditor.[18] The court noted that defendant provided no explanation why each recipient was provided with a copy of the report and whether the disclosures were for a business purpose or to prepare for litigation.[19]

Choosing not to stand up a two-track investigation does not mean that the entirety of the consultant's work would be discoverable. For example, the court in *In re Samsung Customer Data Security Breach Litigation* determined that a consultant's memorandum prepared solely for counsel's use was privileged.[20] Moreover, there would seem to be no reason why an incident response team could not share its non-privileged findings to the privileged investigation workstream. As long as privileged materials are withheld from the response team, such a course could preserve the privileged nature of the report for which counsel engaged the consultant.

Conclusion

While it may be understandable for a company not to prioritize maintaining privilege in the midst of a data breach crisis, it would be good for the company to understand the value of the asset it may be putting at risk. Breach litigation may be ongoing years after the company's incident response team has remediated the company's data system. The company may ultimately regret not taking more proactive steps during the crisis.

Notes:

[1] For a discussion of these decisions and cyber consultants generally, *see* David M. Greenwald, Michele L. Slachetka & Caroline L. Meneau, Testimonial Privileges § 1:30.50 (West 2025).

[2] *Id.* at § 1:29.

[3] *In re Grand Jury,* 23 F.4th 1088, 1092 (9th Cir. 2022) (adopting the primary purpose test for dual purpose communications), *dismissing certiorari as improvidently granted by In re Grand Jury,* 143 S. Ct. 543 (2023).

[4] *See In re Kellogg Brown & Root, Inc.,*756 F.3d 754, 757-60 (D.C. Cir. 2014) (establishing the *a* primary purpose test in the D.C. Circuit). *See also In re General Motors LLC Ignition Switch Litig.,* 80 F. Supp. 3d 521, 530 (S.D.N.Y. 2015) (applying the *a* primary purpose test).

[5] *In re Samsung Customer Data Security Breach Litigation,* 2024 WL 3861330, at *12 (D.N.J. Aug. 19, 2024).

[6] CISA, 6 U.S.C.A. 1501 et seq., includes a privilege safe harbor that provides that provision of cyber threat indicators and defensive measures to the Federal Government will not constitute a waiver of any applicable privilege or protection provided by law, including trade secret information. 6 U.S.C.A. 1504(d)(1).

[7] MDL No. 14-2522 (PAM/JJK), 2015 WL 6777384 (D. Minn. Oct. 23, 2015).

[8] PSACV 15-01592 AB (DFMx), 2017 WL 4325583, at *2 (C.D. Cal. May18, 2017).

[9] 2017 WL 4325583, at * 2. *See also* Testimonial Privileges at § 2:18.

[10] Civil Action No. 20-12198-LTS, 2021 WL 8323636 (D. Mass. June 2, 2021).

[11] 2021 WL 8323636, at *4.

[12] *See* Testimonial Privileges at § 1:131, n. 22.

[13] *See In re Premera Blue Cross Customer Data Sec. Breach Litig.,* 296 F. Supp. 3d 1230, 1245 (D. Or. 2017); *In re Dominion Dental Services USA, Inc. Data Breach Litig.,* 429 F. Supp. 3d 190, 195 (E.D. VA 2019); *Leonard v. McMenamins Inc.,* Case No. C22-0094-KKE, 2023 WL 8447918, at *3 (W.D. Wash. Dec. 6, 2023); *In re Samsung,* 2024 WL 3861330, at *15.

[14] 5296 F. Supp. 3d at 1245.

[15] *Id.; see also Leonard,* 2023 WL 8447918, at *3 ("It is well-established that mere delegation of business functions to an attorney is insufficient to shield otherwise unprotected factual investigation from discovery.").

[16] 2020 WL 2731238, at *1.

[17] *See In re Samsung,* 2024 WL 3861330, at *13; *In re American Medical Collection Agency, Inc. Data Sec. Breach Litig.,* MDL No. 2094, 2023 WL 8595741, at *7 (D. N.J. Oct. 16, 2023); *OTR Transp., Inc. v. Data Interfuse, LLC,* Case No. 21 cv 3415, 2022 WL 296056, at *3 (N.D. Ill. Feb. 1, 2022); *In re Dominion,* 429 at 191-92.

[18] 2020 WL 2731238, at *2.

[19] *Id.*

[20] 2024 WL 3861330, at *16.