Privacy Alert: Work Product Protection for Initial Data Breach Investigations Can Be More Limited Than You Think

Related Professionals

Eric W. Richardson

Jacob D. Mahle

J.B. Lind

Brent D. Craft

Related Services

Data Strategy, Privacy and Security

CLIENT ALERT | 6.1.2020

A recent decision out of the Eastern District of Virginia casts doubt on the scope of work product protection for data breach investigations. On May 26, 2020, Magistrate Judge John F. Anderson, United States District Court for the Eastern District of Virginia, issued a lengthy decision analyzing the work product protection for data breach investigations, in the case of *In re Capital One Consumer Data Sec. Breach Litig.*, No. 1:19MD2915 (AJT/JFA), 2020 WL 2731238 (E.D. Va. May 26, 2020).

In the decision, the court rejected an argument of work product protection and granted a motion to compel production of an initial data breach investigation report prepared by a cybersecurity investigator, FireEye, Inc., d/b/a Mandiant (Mandiant), at the direction of the breached entity's outside counsel. The relevant facts include:

- In March 2019, the breached entity experienced a cybersecurity incident whereby its customers' personal information was compromised.
- On July 19, 2019, the breached entity confirmed that a data breach had occurred.
- On July 20, 2019, the breached entity retained outside counsel to advise it regarding the data breach.
- On July 24, 2019, the breached entity and its outside counsel signed a Letter Agreement with Mandiant whereby Mandiant agreed to provide services and advice concerning "computer security incident response; digital forensics, log, and malware analysis; and incident remediation."
- The Letter Agreement provided that Mandiant's services and payment would be governed by the applicable terms in a Statement of Work and Master Services Agreement that were signed between the breached entity and Mandiant before the breach.
- Although subject to the same terms as the prior MSA and SOW, the Letter Agreement provided that the **work would be done at the direction of outside counsel and the deliverables would be provided to outside counsel instead of the breached entity**.

- On September 4, 2019, the Mandiant Report was issued.
- Mandiant's fees for the data breach investigation were paid initially out of a retainer it had been previously provided under a SOW, and later by the breached entity through its budget for cyber matters.
- In December 2019, Mandiant's fees related to the data breach were re-designated as legal expenses and deducted against the breached entity's legal department budget.
- The Mandiant Report was initially sent to outside counsel, which in turn provided the report to the breached entity's "legal department," the breached entity's Board of Directors, approximately fifty of the breached entity's employees, four regulators (Federal Deposit Insurance Corporation, Federal Reserve Board, Consumer Financial Protection Bureau, and Office of the Comptroller of the Currency), and an accounting firm (Ernest & Young).
- According to the court, there was no explanation provided as to why each recipient was provided with a copy of the Mandiant Report and whether the disclosure was related to a business purpose or for the purposes of litigation. Further, the court stated that, even for those within the breached entity's legal department, it was unclear if they were provided with the Mandiant Report in relation to duties involving the litigation or for regulatory or other business reasons. Lastly, the court stated that it was unclear from the briefing what, if any, restrictions were placed on those persons and entities who received a copy of the Mandiant Report on discussing, copying, or providing the Mandiant Report, or any portion of it, to others.

The plaintiffs moved to compel production of Mandiant's report and the breached entity objected that the report was work product. The court rejected this assertion, concluding that:

- The fact that there is litigation does not, by itself, cloak materials with work product immunity. Rather, "the material must be prepared **because** of the prospect of litigation." *In re Capital One*, 2020 WL 2731238 at *3 (citing *National Union Fire Ins. Co. v. Murray Sheet Metal Co.*, 967 F.2d 980, 984 (4th Cir. 1992)). "Materials prepared in the ordinary course of business or pursuant to regulatory requirements or for other non-litigation purposes are not documents prepared in anticipation of litigation." *In re Capital One*, 2020 WL 2731238 at *3.

- Rather, Magistrate Judge Anderson concluded that work product protection applies "when the party faces an actual claim or a potential claim following an actual event or series of events that reasonably could result in litigation **and** the work product would not have been prepared in substantially similar form but for the prospect of that litigation." *Id.* (citing *RLI Ins. Co. v. Conseco, Inc.*, 477 F. Supp. 2d 741, 748 (E.D. Va. 2007)) (emphasis in original).
- Although agreeing that "there was a very real potential that [the breached entity] would be facing substantial claims following its announcement of the data breach," the court concluded that the "determinative issue is whether the Mandiant Report would have been prepared in substantially similar form but for the prospect of that litigation." *In re Capital One*, 2020 WL 2731238 at *4.
- Magistrate Judge Anderson concluded that the Mandiant Report would have been prepared in substantially the same form, regardless of the litigation. The court concluded that "**the fact that the investigation was done at the direction of outside counsel and the results were initially provided to outside counsel, does not satisfy the 'but for' formulation**." *Id.* (emphasis added).

In support of its conclusion, the court pointed to:

- The breached entity's "long-standing relationship" and "pre-existing SOW with Mandiant to perform essentially the same services that were performed in preparing the subject report";
- "The retainer paid to Mandiant was considered a business-critical expense and not a legal expense at the time it was paid";
- The disclosure of the report to "four different regulators and to [the breached entity's] accountant," the use of the "independent investigation … internally for Sarbanes Oxley disclosures," and the reference to the report in "a draft FAQs prepared by a senior vice president for finance prior to the public announcement of the data breach" show that the "results of an independent investigation into the cause and the extent of the data breach was significant for regulatory and business reasons";
- Although the Mandiant Report was prepared at the direction of outside counsel and initially delivered to outside counsel, "Mandiant issued a written report detailing the technical factors that allowed the criminal hacker to penetrate [the breached entity's] security. There is no statement by [the breached entity], or evidence upon which one could find, that [the breached entity] would not have called upon Mandiant to perform the services described in the SOW that existed prior to the data breach and prepare a written report as provided in the SOW that would have detailed the results of its investigation…." *In re Capital One*, 2020 WL 2731238 at *4.

***

Companies seeking to protect the confidentiality of their initial breach investigations should be careful to observe the formalities that the district court scrutinized in *In re Capital One*. Companies should (1) pay attention to how the forensic investigator's services are compensated by the business and characterized internally – either as a legal expense or as a business expense; (2) control the disclosure of the investigator's report and its conclusions (*i.e.*, clearly instruct recipients that it is legal work product that must be kept confidential); (3) not disseminate the report to an employee or even an in-house attorney unless that dissemination is consistent with the purposes of the attorney work product protection; (4) in any fight regarding attorney work product protection, be able to explain how the report would not have been prepared in substantially similar form but for the threat of litigation; and (5) consider modifying the Statement of Work to provide that the work was to be performed under the direction of counsel, and/or executing a new and separate SOW that clearly identifies the services to be provided as work product to be completed at the direction of counsel.

If you have questions about the scope of work product protection for your company's breach investigation, please contact a member of the Vorys cybersecurity team: Eric W. Richardson, Jacob D. Mahle, JB Lind or Brent D. Craft.