Published on *The National Law Review* https://natlawreview.com

Federal Court Finds Cybersecurity Forensic Report Not Privileged Under Attorney Work Product Doctrine

Article By:

Caressa D. Bennet

Michael R. Bennet

Marjorie Spivak

The United States District Court for the Eastern District of Virginia (Court) has held that a cyber-forensic investigation report was not protected by the attorney work product doctrine and ordered Capital One to produce it in a multidistrict litigation arising out of a 2019 cyber incident.[1]

Bottom Line: *This opinion makes clear that organizations must be careful when hiring cyber forensic companies in anticipation of future litigation. It is critical for organizations to consider when cyber forensic companies should be retained, how they are retained, how they are paid, and how their work will be used and shared both within and outside an organization. If done properly, attorney client privilege and the attorney work product doctrine can be used to shield communications companies from liability in the event of a lawsuit arising from a cybersecurity breach.*

Introduction

In March of 2019, Capital One experienced a data breach whereby an unauthorized person gained access to personal information relating to Capital One customers. On July 29, 2019, Capital One issued a public announcement concerning the data breach. Numerous law suits were filed against Capital One. The subject opinion is the result of a plaintiffs' motion to compel production of a cyber-forensic report which detailed the technical problems that allowed a bad actor to breach Capital One's network. Capital One argued that the report was protected by the attorney work product doctrine because it was requested by a law firm and prepared in anticipation of litigation following Capital One's March 2019 data breach. The Court disagreed based on the facts which showed that the law firm was engaged to work with Capitol One after the breach occurred. Had the law firm been properly retained prior to the breach and hired the cybersecurity firm to work at its direction rather than the company's, the attorney client privilege and attorney work product doctrine would have remained in place.

Background

Beginning in November of 2015, Capital One entered into a Master Services Agreement (MSA) with FireEye, Inc. d/b/a Mandiant (Mandiant) and Statements of Work (SOW) for cybersecurity incident response support. Capital One paid Mandiant a retainer for a January 2019 SOW which entitled Capital One to 285 hours of services from Mandiant. Capital One designated the retainer paid to Mandiant as a business critical expense, not a legal expense. The 2019 SOW required Mandiant to provide computer security incident response support, digital forensics, log and malware analysis support, and incident remediation assistance. Under the agreements, Mandiant would provide a detailed report covering the activities, results and recommendations for remediation.

Following the March 2019 data breach, Capital One retained Debevoise & Plimpton (Law Firm) to provide legal advice in connection with the data breach incident. On July 24, 2019, the Law Firm signed a Letter Agreement with Mandiant for services including computer security incident response, digital forensics, log and malware analysis, and incident remediation. The Letter Agreement provided that payment terms and services were to be the same as those in the 2019 SOW and 2015 MSA between Capital One and Mandiant; however, the work would be done at the direction of counsel with the deliverables provided to counsel instead of Capital One.[2] Had the law firm been retained prior to the breach and directly engaged and paid Mandiant to do the work, the attorney-client privilege and attorney work product doctrine would be preserved. Instead, Mandiant performed the services outlined in the Letter Agreement and issued a report (Mandiant Report) on September 4, 2019 that detailed the technical factors that allowed the criminal hacker to penetrate Capital One's security. Mandiant was paid for its work out of the retainer already provided by Capital One under the 2019 SOW. After the retainer was exhausted, additional fees were paid directly by Capital One through its cyber budget. In December 2019, the Mandiant expenses relating to the data breach were re-designated as legal expenses. The Mandiant Report was initially sent to the Law Firm, which in tum, provided the report to Capital One's legal department, Capital One's Board of Directors, fifty Capital One employees, an accountant, and four regulators.

The Plaintiffs sought release of the Mandiant Report arguing that it was prepared for business and regulatory purposes and therefore not privileged. Capital One argued that it was privileged because it was prepared in anticipation of litigation. The Court disagreed and ordered Capital One to release the Mandiant Report finding it not covered by the work product doctrine.

Law

The Court explains that the party asserting the work product doctrine bears the burden of demonstrating the applicability of that doctrine.[3] The Court also notes that courts in general disfavor assertions of evidentiary privileges because they shield evidence from the truth-seeking process and therefore must be narrowly construed.[4] The Court next explains that the Federal Rule of Evidence 502 defines work-product protection as '"the protection that applicable law provides for tangible material (or its intangible equivalent) prepared in anticipation of litigation or for trial."[5] Citing the Fourth Circuit, the Court clarifies that the fact 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.[6] Materials prepared in the ordinary course of business or pursuant to regulatory requirements or other non-litigation purposes *are not* documents prepared in anticipation of litigation.[7] In designing Womble Bond Dickinson’s Cybersecurity Incident Response Retainer, we structured it with an eye always to eventual litigation arising out of a cybersecurity breach.
The Capital One case emphasizes the need to have the law firm directing the breach incident response as well as the steps taken by the company ahead of the breach to ensure its network is secure and risks for breach are mitigated as much as possible.

According to the Court, for a document to be entitled to protection, a court must determine the driving force behind the preparation of a requested document.[8] The "because of" standard is designed to protect only work that was conducted because of the litigation and not work that would have been done in any event.[9] The Court states that the work product doctrine does not protect documents that would have been created in essentially similar form irrespective of the litigation. Thus, the 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. Again, this illustrates why it is critically important to have the attorney directing the process prior to a breach occurring in anticipation of litigation that will result after a breach occurs. Vulnerability scans, penetration tests, network monitoring and all of the reports and discussions taking place should involve and be directed by counsel without the taint of the information being shared with third parties not hired through counsel.

Opinion

In rejecting Capital One's contention that the Mandiant Report was privileged, the Court found that Capital One failed to show that "but for" the prospect of litigation, the report would not have been prepared in substantially the same form. In short, the Court concludes that the report, because the investigation was done at the direction of outside counsel hired after the breach occurred and because the results were initially provided to outside counsel, does not satisfy the "but for" test. According to the Court, Capital One failed to present evidence to show that the Mandiant Report would not have been done in substantially similar form even if there was no prospect of litigation.

The Court bases its conclusion on several factors. First, Capital One had a long-standing relationship with Mandiant and a pre-existing SOW with Mandiant to perform essentially the same services that were performed in preparing the subject report. While the Court finds no question that at the time Mandiant began its incident response services in July 2019, there was a very real potential for litigation, the Court frames the determinative issue as whether the Mandiant Report would have been prepared in substantially similar form but for the prospect of that litigation. The Court also notes that the retainer paid to Mandiant was considered a business critical expense at the time it was paid. In addition, the fact that the Mandiant Report was provided to four different regulators and Capital One's accountant shows that it was significant for regulatory and business reasons. The sharing of the report with these third parties even had it been prepared at the direction of counsel and even had Mandiant been working for the attorneys would have caused the attorney-client privilege to be lost. To keep the attorney-client privilege in place and to fall under the attorney work product doctrine, information between the company and its attorneys cannot be shared with third parties. Once that occurs, the privilege is lost.

Further, the Court found that the only evidence presented that the Mandiant Report was prepared for litigation is that the work was requested at the direction of, and delivered to, outside counsel. However, the Court explains that the work as set out in the SOW and Letter Agreement to be performed by Mandiant was the same. According to the Court, the retention of outside counsel after the breach occurs does not, by itself, turn a document into work product. The Court concludes that Capital One did not carry its burden of showing that Mandiant's scope of work under the Letter Agreement with outside counsel was any different than the scope of work outlined in the existing SOW, or that the work would not have been performed without the prospect of litigation. The Court therefore ordered Capital One to produce the Mandiant Report.

Conclusion

This opinion is a critical reminder that organizations must consider in advance how to hire, pay, and utilize a cyber-forensic service provider. Courts are taking a hard look as to whether to afford protection to the work of cyber incident response service providers.[10] While this decision stands in conflict with previous court cases that apply a more flexible standard, it is important to understand the factors that led to the subject opinion. The Court emphasized the prior relationship between Capital One and Mandiant dating back to 2015, with an SOW signed in 2019, prior to the breach. The Court also considered the nature of Mandiant's work to be substantially similar to work that was done without layering in the prospect of litigation. In fact, the Court noted the only difference in Mandiant's work post breach was that it was done at the direction of counsel, which did not alter the business purpose of the work. That is why it is critical to work with counsel early in the process so that it is clear that the cybersecurity work being performed to identify, protect, detect, respond and recover is being undertaken to reduce liability to the company after a breach occurs and the company is sued. The Court also found suspect the fact that Capital One paid for Mandiant's work as a business critical expense, rather than a legal expense, since it was paid for out of the existing 2019 SOW retainer, and then through Capital One's cyber budget (and subsequently re-labeled a legal expense). Accordingly, any cybersecurity retainer paid to our firm should always be accounted for as a legal expense. Finally, the Court viewed the disclosure of the Mandiant Report to numerous parties both inside and outside the organization as evidence that the report was for business or regulatory purposes rather than litigation. As discussed earlier, sharing confidential attorney work product with third parties will result in loss of the protection. We advise our clients to only share such information with employees on a need to know basis.

---

[1] *In Re: Capital One Consumer Data Security Breach Litigation*, MDL No. 1:19md2915 (AJT/JFA) (May 26, 2020).
[2] On July 26,2019, an addendum to the Letter Agreement was prepared to include penetration testing of systems and endpoints.
[3] *Solis v. Food Employers Labor Relations Ass'n*, 644 F.3d 221, 232 (4th Cir. 2011); *Sandberg v. Virginia Bankshares, Inc.*, 979 F.2d 332,355 (4th Cir. 1992).
[4] *In re Grand Jury Proceedings*, 727 F.2d 1352, 1355 (4th Cir. 1984), *RLI Ins. Co. v. Conseco, Inc.*, 477 F. Supp. 2d 741, 748 (E.D. Va. 2007).
[5] Fed. R. Evid. 502(g)(2).
[6] *National Union Fire Ins. Co. v. Murray Sheet Metal Co.*, 961 F .2d 980 (4th Cir. 1992),
[7] *Id*.
[8] *Id*.
[9] *Id*. at 747.
[10] *See In re Dominion Dental Servs. USA, Inc. Data Breach Litig.*, 429 F. Supp. 3d 190 (E.D. Va. 2019); *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 296 F. Supp. 3d 1230 (D. Or. 2017).

National Law Review, Volumess X, Number 164