JUNE 26, 2020

Data Breach Class Actions – Eastern District of Virginia Finds Cybersecurity Firm Incident Report Not Protected by Work-Product Doctrine

by Jeffrey H. Fisher

Takeaway: Counsel for companies that suffer a data breach often hire an outside cybersecurity firm to remediate the breach and assist counsel in preparing for and defending against litigation. These companies typically take the position that the cybersecurity firm's report constitutes attorney work-product not subject to discovery because it was prepared for counsel in anticipation of litigation. But a Magistrate Judge in the Eastern District of Virginia ordered Capital One to produce such a report, finding that the report was not created primarily for litigation. *In re Capital One Consumer Data Sec. Breach Litig*., 1:19MD2915 (AJT/JFA), 2020 WL 2731238, at *1 (E.D. Va. May 26, 2020),

The fact pattern in *Capital One* is familiar. Capital One suffered a data breach in March 2019. In July 2019, after it discovered the breach, Capital One retained Debevoise & Plimpton LLP. To assist in its investigation, Debevoise signed an agreement with Mandiant, a cybersecurity firm that had already been providing cybersecurity services to Capital One. The agreement provided that Mandiant's work would be at the direction of counsel and that its report and any other deliverables would be provided directly to Debevoise, as opposed to Capital One. Mandiant issued its report in September 2019 ("Mandiant Report").

Following its announcement of the data breach, Capital One was hit with a slew of data breach actions. The cases were ultimately consolidated in the Eastern District of Virginia. In April 2020, the plaintiffs moved to compel production of the Mandiant Report, arguing that it was not protected by the work-product doctrine because it was commissioned and used for a business purpose and not solely for litigation.

In a carefully-reasoned opinion that analyzed numerous cases addressing work-product protection over cybersecurity reports, the Magistrate Judge granted the plaintiffs' motion to compel. The court determined that, for the report to receive work-product protection, Capital One bore the burden of showing that the report was "prepared 'because of' the prospect of litigation," and that litigation was "the driving force behind the preparation" of the report. 2020 WL 2731238, at *3. Certain key facts demonstrated that Capital One could not satisfy the "because of litigation" standard.

First, Capital One had a longstanding relationship with Mandiant, and Mandiant had been performing cybersecurity services for Capital One for years prior to the data breach. Although Mandiant entered into a "new" agreement with Debevoise, the services identified in that agreement were identical to services contemplated in Mandiant's original, pre-litigation agreement with Capital One. Indeed, Capital One classified the retainer paid to Mandiant as a "business-critical expense," not a legal expense.

Second, the Court found that the Mandiant Report was not used only for litigation purposes. After

Mandiant sent the report to Debevoise, the Report was shared with at least 51 Capital One employees and four regulators (the Federal Deposit Insurance Corporation, the Federal Reserve, the Consumer Financial Protection Bureau, and the Office of the Comptroller of the Currency), as well as Capital One's accounting firm, Ernst & Young. The court noted that Capital One planned to use the report to show the breach had no impact on its financial accounting controls, as well as to make disclosures under Sarbanes-Oxley. Capital One also shared the report with technical employees, who reviewed the report to help understand and respond to the data incident.

The *Capital One* decision demonstrates that simply having outside counsel engage and direct the work of a third-party cybersecurity firm is not sufficient to ensure work-product protection, because courts look holistically at the purpose and nature of the engagement. If a defendant wants to avoid disclosure of a cybersecurity report in litigation, it should ensure that the report is created and used solely for the purpose of the litigation.

This creates challenges for data breach victims. Although it makes financial and practical sense to engage one firm to create one report that can be used for remediation, compliance, and litigation purposes, *Capital One* shows that this approach creates a risk of disclosure. If possible, defendants should consider either hiring a separate firm to conduct a litigation analysis or having its primary cybersecurity firm create two, separate reports – one for litigation purposes and one for remedial and regulatory purposes. Defendants must also carefully limit who in the company (and outside the company) receives the litigation report.

The public policy underlying the decision also merits discussion. There is, of course, good reason to encourage companies hit with a data breach to hire sophisticated cybersecurity firms that will help them understand the scope of the data breach and prevent future attacks. But a thorough analysis is also likely to identify security deficiencies that can be used against the victim in litigation. The *Capital One* court implicitly determined that the importance of full disclosure in discovery outweighed any negative impact the decision would have concerning the retention of cybersecurity experts.

Although others courts have denied similar motions to compel, *Capital One* demonstrates that data breach victims cannot assume that cybersecurity reports will not be produced and should be careful to limit the use and distribution of the report. Capital One has filed objections to the Magistrate Judge's order under Federal Rule of Civil Procedure 72, so the District Court will take a second look at this issue.