TRAUB LIEBERMAN

CYBER LAW BLOG

June 16, 2020

Virginia Federal Court Rejects "Work Product" Protection for Forensic Report Prepared in Capital One Data Breach Litigation

BY: Jason Taylor

When a data breach occurs, the affected company (or preferably its counsel) will retain a data security or forensics firm to investigate the breach and prepare a report. Forensic reports of a data breach typically identify the likely method by which the hacker accessed a company's data, exposing critical vulnerabilities in its systems. The forensic report may also identify areas in which a company failed to maintain industry standards or to maintain its contractual or other obligations to protect clients and employees' information. When properly prepared, these reports are privileged from disclosure in subsequent litigation based on protections afforded by the "work product" doctrine or similar privileges. However, such privileges are not absolute as demonstrated by a recent Virginia federal court decision ordering production of a forensic report prepared in connection with the infamous Capital One data breach that occurred last year. *See In Re: Capital One Consumer Data Security Breach Litigation,* 2020 WL 2731238 (E.D. Va. May 26, 2020).

By way of background, in March 2019 Capital One experienced a data breach whereby an unauthorized person gained access to certain types of personal information affecting over 100 million Capital One customers. On July 29, 2019, Capital One issued a public announcement concerning the data breach, and the following day the first of many lawsuits were filed against the company asserting claims based on the data breach. Capital One confirmed that a data breach had occurred on July 19, 2019, and retained Debevoise & Plimpton ("Debevoise") to provide legal advice in connection with the data breach incident the next day.

On July 24, 2019, Debevoise and Capital One 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." Notably, Capital One had previously entered into a Master Service Agreement with Mandiant in November 2015 to provide periodic computer security and forensic work for Capital One. In January 2019, Madiant executed a statement of work to perform computer and data security services for Capital One. Mandiant preformed the services that had been outlined in the Letter Agreement and prepared a report "detailing the technical factors that allowed the criminal hacker to penetrate Capital One's security." The Mandiant Report was issued on September 4, 2019.

Plaintiffs in the data breach litigation sought to compel production of the Mandiant Report and related materials. Capital One objected claiming that the report was privileged and protected from disclosure by the "work product" doctrine. 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." Fed. R. Evid. 502(g)(2). Generally, the fact that there is litigation does not, by itself, shield materials with work product immunity; rather the material must be prepared *because of* the prospect of litigation. 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 order to be entitled to protection, a document must be prepared "because of" the prospect of litigation and the court must determine "the driving force behind the preparation of each requested document" in resolving a work product immunity question. *In Re: Capital One Consumer Data Security Breach Litigation,* 2020 WL 2731238 at *6.

According to the District Court, 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. The work product doctrine does not protect documents that would have been created in essentially similar form irrespective of the litigation. *Id.* In other words, 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.

The District Court found no question that at the time Mandiant began its "incident response services" in July 2019, there was a very real potential that Capital One would be facing substantial claims following its announcement of the data breach. According to the District Court, the determinative issue was whether the Mandiant Report would have been prepared in substantially similar form but for the prospect of that litigation. Ultimately, the court found that Capital One failed to meet its burden to show that Mandiant's incident response services would not have been done in substantially similar form even if there was no prospect of litigation.

Initially, the District Court reasoned that the hiring of outside counsel does not excuse a company from conducting its duties and addressing business issues related to the company. The mere fact that the investigation was done at the direction of outside counsel and the results were initially provided to outside counsel, did not satisfy the "but for" formulation discussed above. One significant fact relevant to the District Court was that Capital One had an *existing* statement of work and MSA with Mandiant at the time of the data breach that was effectively transferred to outside counsel. The statement of work predating the breach was the same as that provided under the Letter Agreement. In other words, the work to be performed by Mandiant was the same, the terms were the same, but the only difference was that the work was to be performed at the direction of outside counsel and the final report delivered to outside counsel. The retainer paid to Mandiant was also considered a business-critical expense and not a legal expense at the time it was paid.

As a final lesson, the District Court found that the retention of outside counsel, by itself, did not turn a document into work product. The report was eventually disclosed to at least several members of Capital One's cyber technical, enterprise services, information security and cyber teams, regulators, and accountants (over 50 people in all), without explanation as to why each recipient was provided a copy of the report and whether the disclosure was related to a business purpose or purposes of litigation. The court noted that the report was also used by Capital One for various business and regulatory purposes, and that the company presented no evidence to conclude that Mandiant's services would not have been the same but for the breach. The court reasoned that Mandiant's services prior to the data breach would have likely included or identified the same technical factors that allowed the hacker to penetrate Capital One's security, which were likely determined in connection with the breach report.

In the end, the court found that Capital One presented insufficient evidence to justify protection under the “work product” doctrine, granting plaintiffs’ motion to compel production of the Mandiant Report. The decision highlights some of the difficulties large companies have in protecting their investigation of data breach events, and it also provides some lessons for companies and counsel in how to ensure that forensic reports remain protected. Namely, retain counsel early, limit disclosure of any forensic report to the companies legal team only where possible, and ensure that preparation of any documents or reports are for purposes of litigation only.