CYBERSECURITY, PRIVACY AND DATA PROTECTION ALERT

Capital One and the Attorney Work Product: How To Protect Breach Reports

By: Daniel S. Marvin

We recently reported on the decision of *In Re: Capital One Consumer Data Security Breach Litigation,* MDL No. 1:19md2915 (AJT/JFA)(E.D. Va.), in which a Federal District Court found that a report prepared by cybersecurity consulting firm Mandiant (at the direction of counsel) in the wake of a data breach at Capitol One was *not* protected under the work product doctrine, and must therefore be turned over to Plaintiffs. As someone who has been litigating for about 20 years, I am generally affronted by any incursion into the attorney work-product doctrine, which has been engrained in our system of jurisprudence since the Supreme Court's 1946 ruling in *Hickman v. Taylor*. However, since my personal feelings don't matter much to the courts, there are some takeaways and lessons to be learned from the *Capital One* decision which could help your organization preserve the work-product doctrine should the need arise.

The important facts of *Capital One* are as follows: In November 2015, Capital One entered into a Statement of Work (SOW) with cybersecurity consultant Mandiant, for among other things, services responding to cybersecurity incidents. In January 2019, Capital One entered into another SOW with Mandiant for 285 hours of incident response services (designating it a "Business Critical" expense rather than a "Legal" expense). In July, 2019, Capital One announced the data breach. Subsequently, Capital One and its outside counsel signed a Letter Agreement with Mandiant to perform the services set forth in the SOW, but at the direction of outside counsel. On September 4, 2019, Mandiant issued a report on the vulnerabilities that allowed a criminal hacker to penetrate Capital One's security. Capital One, upon being sued, refused to produce the report based upon the attorney-work product doctrine and a dispute arose.

MORRISON MAHONEY LLP

The Court found that despite "the very real potential that Capital One would be facing substantial claims," the breach report had to be produced because it would have been prepared in substantially similar form (pursuant to the prior SOW) even without the prospect of litigation. Further, the mere facts that the investigation was done at the direction of outside counsel, and that the report was sent directly to counsel once complete, did not satisfy the Court that it was produced solely in anticipation of litigation. In other words, because of the prior SOW, the report had dual purposes – business and legal – and the dual purpose eradicated the work-product doctrine. Notably, as the *Capital One* Court pointed out, there are other court decisions which, under different factual scenarios, have protected consultant breach response reports from production. In that regard, *Capital One* seems to be a worst-case scenario for those looking to preserve consultant reports as work-product, but it a scenario that no litigant wants to face. So here are a few things to do to avoid a similar fate.

First, have outside counsel retain the consultant. If the consultant has a pre-existing relationship with the company, enter into a new agreement setting forth new responsibilities given anticipated ligation. These duties will generally revolve around being guided by and directed by counsel, as well as around the format of the report and to whom it should be sent. Importantly, none of these new obligations should be included in any prior agreements.

Second, and at the risk of stating the obvious: *actually have the breach report drafted at the direction of counsel*. This means more than having counsel make the request that it be prepared and turned over to him or her once complete. Outside counsel needs to be actively involved in directing the report, steered by the knowledge that data breach litigations typically involve the same claims: negligence, breach of contract and violations of state law data privacy or consumer protection statutes. Once a breach occurs, outside counsel should quickly evaluate the facts and provide detailed guidance to the security consultant as to what specific factual things to include in the report in order to speak to, among other things, (i) the reasonableness of the security controls in place given the risk which was faced and now encountered, (ii) the mistakes made by employees or contractors which could give rise to liability, as well as (iii) the potential injury faced by any affected persons.

For example, in law school, attorneys are taught the elements of a negligence claim: duty, breach, proximate cause, direct cause and damages. Given those elements, outside counsel should explain to the consultant what the organization's duties were with respect to securing the systems or data which have been compromised, what facts to look for in terms of a breach of that duty and what effect the breach had on the company and its protected information. Importantly, the consultant should *not* be asked to speak to if there was a duty or if a breach of

that duty occurred, but merely to present the facts which outside counsel feels are needed to evaluate those elements. The same holds true for breach of contract claims and state statutory claims; counsel should examine any applicable contracts and statutes and advise the consultant on what facts to look out for given the organization's contractual or statutory obligations. In other words, counsel should be *active* and not *passive*. The *Capital One* decision didn't discuss counsel's involvement in the preparation of the report at issue, but it was likely little to none (or else it would have been discussed), and that was surely a dispositive factor.

Third, if a report is also needed for business purposes, it should be prepared separately and pursuant to the pre-existing SOW, and should also be different than the report prepared in anticipation of litigation (or perhaps a redacted version). Payment for a secondary report should be made pursuant to the pre-existing SOW (out of business funds) while payment for the litigation report should be made out of legal spending (assuming your organization is set up that way).

Finally, the completed report should be sent to counsel, and counsel only should be responsible for its dissemination to others. Simple enough.

By following these few tips, as well as the advice of your counsel, you should be well on your-way to providing the shield of work-product protection to post-breach consultant reports.