

Maintaining Privilege and Work Product Protections in Dual Purpose (Legal and Business) Investigations

Minding Your Business Blog on June 1, 2020

Requires More than Merely Adding Counsel's Name to a Forensic Report.

Technical investigations conducted following cyber-incidents often have both legal and ordinary-course business purposes. In certain jurisdictions, reports generated as a result of such investigations can be protected from discovery by privilege and work product protections— despite certain non-legal use – under the “dual purpose” doctrine when “consider[ing] the totality of the circumstances . . . it can fairly be said that the document was created because of anticipated litigation and would not have been created in substantially similar form but for the prospect of litigation.” [California Earthquake Auth. v. Metro. West Sec. LLC](#). However, as a recent opinion illustrates, dual purpose-type privilege claims may not be upheld if challenged in the absence of proper precautions. [In re: Capital One Customer Data Sec. Breach Litig., MDL No. 1:19-md-02915, D.I. 490, Slip Op. \(E.D. Va. May 26, 2020\) \(“Slip Op.”\)](#).

In July 2019, Capital One learned that a hacker accessed and stole highly sensitive customer information from Capital One’s online cloud environment (the “Breach”). [Mem. In Support of Mot. To Dismiss Representative Consumer Class Action Complaint](#). It was ultimately discovered that the Breach compromised more than 100 million customers’ information.

Following the initial detection of the intrusion, Capital One hired outside counsel to investigate and help the company prepare for anticipated litigation and regulatory inquiries. To assist counsel's investigation, outside counsel engaged a cybersecurity consultant. Capital One used this same consultant prior to the Breach in the normal course of its business. Instead of operating under the pre-existing Master Services Agreement ("MSA") between consultant and Capital One, outside counsel entered into a new Letter Agreement with the consultant. Slip Op. at 2. The new Letter Agreement included the same description of services as the services specified in the earlier MSA, but specified that the work would be done at the direction of counsel. Further, any deliverables would be provided to outside counsel instead of to Capital One. *Id.* at 2-3.

The cybersecurity consultant investigated the intrusion, prepared a forensic report regarding the Breach (the "Report"), and delivered it to outside counsel. *Id.* at 4. Outside counsel then provided the Report to Capital One's legal department and Capital One's Board of Directors. *Id.* The Report was eventually disclosed to "approximately fifty Capital One 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 (Ernst& Young)." *Id.*

Subsequently, Plaintiffs, Capital One customers whose information was compromised in the Breach, sued Capital One for – among other causes of action – negligence, breach of contract, and violations of consumer protection statutes. During the course of discovery, Plaintiffs moved to compel production of the Report, arguing that the consultant was retained for business purposes, and, accordingly, its resulting Report was discoverable and should not be withheld. [Mem. in Support of Plaintiffs' Mot. to Compel Production of Report and Related Materials](#).

As the party asserting privilege protection, the Court noted that it was Capital One's burden to show that the Report "would not have been prepared in substantially the same form or with the same content" but for the prospect of litigation. Slip Op. 9. The Court ruled that Capital One had not met its burden for two main reasons: 1) Capital One had not presented sufficient evidence to show that the Report would not have been prepared in substantially similar form and with similar content in the absence of litigation; and 2) Capital One had not treated the Report as privileged or protected. *Id.* at 7-8.

The Court found insufficient the fact that the Letter Agreement stated work was to be performed at the direction of outside counsel and the Report given first to outside counsel. *Id.* at 7 (“As in *RLI*, 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.”). More specifically, the Court found significant that:

- Capital One had a long-standing relationship with the cybersecurity consultant and had a pre-existing MSA “to perform essentially the same services that were performed in preparing the subject report.” *Id.* at 7.
- The retainer paid to the cybersecurity consultant for assisting with investigating the Breach “was considered a business-critical expense and not a legal expense at the time it was paid.” *Id.* at 8.
- The Report was “used internally for Sarbanes Oxley disclosures and was referenced in a draft FAQs prepared by a senior vice president for finance prior to the public announcement of the [Breach].” *Id.*
- The Report was disclosed to “at least several members of Capital One’s cyber technical, enterprise services, information security and cyber teams” and it was “used by Capital One for various business and regulatory purposes.” *Id.* at 10.

Accordingly, the Court ordered the production of the report.

The *Capital One* decision should not be read as a broad repudiation of the dual purpose doctrine, but rather, a holding based on the specific circumstances of that case. *Id.* at 10 (“...each case must be determined on its own facts and circumstances...”). However, *Capital One* suggests a number of things that can be done to increase the likelihood that the protections that can be afforded to dual-purpose investigations would better withstand judicial scrutiny:

- Make Sure Counsel is Actively and Integrally Involved - In *Capital One*, the Court notably did not discuss counsel’s substantive involvement in the investigation. Presumably, because outside counsel in that case only had a “passive” role. Indeed, the Court noted that the scope of the investigation performed in *Capital One* (as set forth in the contract entered into with counsel) was identical to the scope of investigations contracted for and performed in the ordinary course. Other courts considering this issue have warned that counsel should have more than a cosmetic role in an investigation to be able to claim privilege and work product protections. See [U.S. v. ISS Marine Serv., Inc.](#) (“Unfortunately for the respondent, this sort of ‘consultation lite’ does not qualify the Audit Report for the protections of

the attorney-client privilege... This sort of arms-length coaching by counsel, as opposed to direct involvement of an attorney, undercuts the purposes of the attorney-client privilege in the context of an internal investigation.”). Given that courts look at the totality of the circumstances, the greater the evidence that outside counsel was actively involved in the investigation, the easier it will be to distinguish the investigation from those that did not involve counsel.

- Consider the Use of Different Consultants/Vendors – Cases that considered this issue prior to *Capital One* have maintained privilege claims even when the work was performed by consultants that had previously done ordinary course work. See e.g., [In re: Bard IVC Filters Prod. Liab. Litig.](#) (“True, there are some similarities between the [earlier] HHEs and the Report, but the documents clearly serve different purposes and their substantial differences corroborate Dr. Lehmann’s testimony that the Report was a different undertaking than the work he did as acting medical director.”). While such practices appear to remain permissible post-*Capital One*, given the burden of proof placed on the party asserting privilege, consideration should be given to whether it would be advantageous to retain a vendor that does not have a pre-existing relationship. While not essential, the use of an “unrelated” vendor might help further distinguish a privileged investigation from those conducted for purely business reasons. However, there may also be circumstances where, for example, prior familiarity with corporate systems is a critical advantage in a fast moving and high stakes investigation. Accordingly, the use of a vendor with such experience may still be justified post-*Capital One*. However, care should always be taken to differentiate the engagement to reduce the likelihood that a court would find that the investigation is of the same essential nature as those normally performed by the business.
- Be Careful Distributing Privileged or Protected Materials – While reports generated as a result of dual purpose investigations can be used for certain business purposes without destroying privilege protections, this is not carte blanche to use and distribute the reports freely. Permissible business use generally relates to the areas where the business and legal purposes intersect. See e.g., [California Earthquake Auth.](#), 285 F.R.D. at 591 (finding that substantial evidence to support a claim of work product protection over documents generated by consultant despite having some business uses because “these corollary business purposes were ‘profoundly interconnected’ with the audit’s litigation purposes”). The provision of the purportedly privileged reports in *Capital One* to third party regulators and auditors is of particular concern, as it could give rise to a claim that the privilege claims were only selectively asserted. If a party does not treat their report as privileged, they cannot expect that the Court will treat the report differently.

How courts handle materials prepared in data breach investigations during discovery is a developing and fact-driven area of law. While these takeaways may help protect materials from dual-purpose investigations, courts will consider all the facts in determining whether a protection or privilege applies. If a party intends for a cyber-investigation to be protected by privilege, it must be properly structured at the very start of the investigation or there is a greater risk that, when challenged, the privilege protections will fail.

[View original](#)

Related Professionals

- **Nolan M. Goldberg**
Partner