SULLIVAN & CROMWELL LLP

June 26, 2020

Federal Court Compels the Production of Cybersecurity Firm's Incident Response Report in *Capital One* Customer Data Security Breach Litigation

Court Rejects Work Product Protection for Report

SUMMARY

On June 25, 2020, a district court in the Eastern District of Virginia upheld a magistrate court's order compelling Capital One to disclose in civil discovery a report prepared by a third party cybersecurity consultant, Mandiant, in the aftermath of the data breach discovered by the bank in July 2019. The court rejected Capital One's claim that because its law firm formally engaged the incident response firm following the breach and the report was delivered to counsel, the report was entitled to work product protection.[1] The court found that Capital One failed to establish that the report would not have been prepared in substantially the same form but for the prospect of litigation. The court cited the fact that Mandiant's services, including preparation of a report, were called for by a pre-existing statement of work ("SOW") between Capital One and Mandiant, and distributed to many non-legal employees of the bank as well as to external auditors and regulators.

The ruling is the latest in a series of cases in which courts have examined attorney-client privilege or work product claims over investigative reports prepared by cybersecurity firms. In light of the *Capital One* opinion, there are several steps that companies may consider taking when preparing for a possible cybersecurity breach that may put them in a better position to claim work product protection over any investigative report created in connection with a breach.

BACKGROUND

On July 19, 2019, Capital One identified an instance of unauthorized access to systems containing personal information associated with its credit card customers and applicants.[2] By the company's estimate, the data breach, which occurred in March 2019, affected approximately 100 million individuals in the United States and 6 million in Canada, and compromised sensitive personal information including social security and bank account numbers.[3]

On July 20, 2019, one day after confirming the incident, Capital One retained external counsel to provide legal advice in connection with the breach, and in turn, on July 24, counsel engaged Mandiant to provide certain incident response, analysis, and remediation services.[4] The engagement letter incorporated by reference all substantive terms and payment arrangements set forth in a pre-existing master services agreement ("MSA") and SOW between Capital One and Mandiant for cyber incident response services, but provided that Mandiant's services in response to this particular breach would be performed at the direction of external counsel and that Mandiant would provide all deliverables (such as a forensic report) to external counsel.[5]

After it announced the breach on July 29, consumer plaintiffs filed dozens of lawsuits against Capital One that were eventually consolidated in the Eastern District of Virginia.[6] Meanwhile, Mandiant prepared a report of its investigation that it provided to external counsel, which report was later shared with Capital One's legal department, Board of Directors, financial regulators, external auditor, and approximately 50 non-legal employees.[7]

Plaintiffs moved to compel the production of Mandiant's report, arguing that it was not entitled to work product protection. On May 26, the magistrate judge granted plaintiffs' motion to compel.[8] The magistrate judge applied the Fourth Circuit's two-part test for determining whether litigation was the "driving force" behind the preparation of a document that serves both business and litigation needs, namely, whether the document is created when litigation is "a real likelihood" and not "merely a possibility," and whether the document would have been created in essentially the same form in the absence of litigation.[9]

In the magistrate court's view, while Capital One satisfied the first prong, it failed to present "sufficient evidence to show that the services performed by Mandiant would not have been done in substantially similar form even if there was no prospect of litigation" and thus failed the test required for the application of the work product doctrine.[10] In particular, the magistrate found that the bank's pre-existing arrangement with Mandiant calling for the same services that external counsel asked Mandiant to provide, and the bank's distribution of the report to dozens of non-legal personnel and external parties, showed that the "driving force" behind the preparation of the report was not litigation.

Capital One sought relief from the order in part on the basis that the magistrate judge's inquiry—whether the Mandiant report would have been created in essentially the same form in the absence of litigation[11]—

was unduly restrictive under Fourth Circuit law. Capital One bolstered its briefing with newly introduced supporting affidavits from internal counsel and a Mandiant representative, and raised the negative policy implications of forcing companies and their counsel to choose between engaging the cybersecurity consultant experienced in the victim company's networks, personnel, and processes, and preserving a viable work product protection claim over any final incident report.[12] Additionally, on June 4, Capital One produced to plaintiffs materials related to two internal investigations undertaken by the bank's cybersecurity department that were distinct from the investigation carried out by Mandiant and external counsel over which the bank asserted privilege.[13]

The district court found that the magistrate judge correctly applied the law, and embraced the magistrate court's reasoning and conclusion that Capital One must produce Mandiant's report. In particular, the court emphasized the existence of the SOW between Mandiant and Capital One that predated the data breach. The court described the bank's contention that "Mandiant changed the nature of its investigation, the scope of work, and its purpose in anticipation of litigation" as "hollow in light of the respective scope of services covered under the Letter Agreement and the 2019 SOW, which are identical."[14] The court also noted that Capital One paid for Mandiant's services from a fund designated for "business critical" expenses, later reclassifying the expenses as legal.[15]

The district court also found it appropriate to consider the report's "post-production distribution" within the bank and to outside auditors and regulators as "probative of the purposes for which the work product was initially produced."[16] "In sum," the court wrote, "Capital One had determined that it had a business critical need for certain information in connection with a data breach incident, it had contracted with Mandiant to provide that information directly to it in the event of a data breach incident, and after the data breach incident at issue in this action, Capital One then arranged to receive through [external counsel] the information it already had contracted to receive directly from Mandiant."[17]

The court considered and dismissed in a footnote Capital One's broader concerns regarding the "unworkable" practical realities imposed on heavily regulated companies by the magistrate judge's order, noting that the argument "ignores the alternatives available to produce and protect work product, either through different vendors, different scopes of work and/or different investigation teams."[18]

IMPLICATIONS

The *Capital One* decision shows the scrutiny that may be applied to work product claims in the cybersecurity context, in which incident reports prepared by cybersecurity firms frequently serve both litigation and business needs. Companies should review their existing arrangements with cybersecurity vendors and external counsel to determine whether they are best positioned to maintain a viable claim of privilege before a court applying similar reasoning.

Although the district court in *Capital One* noted that companies can properly produce and protect work product through different vendors, scopes of work, and/or investigation teams, the practical reality, as Capital One argued, is frequently more complex. There can be significant benefits to having incident response handled by a cybersecurity firm that is familiar with the company's systems as well as considerable downsides to requiring different investigation teams to respond to the breach and to advise external counsel from the inception of the incident. Nonetheless, as companies engage in cybersecurity planning, they should consider the feasibility and desirability of these options. Under certain circumstances and notwithstanding the inconvenience, companies may consider whether their external counsel should retain a different cybersecurity firm—or a walled off team within the same firm—to advise counsel in anticipation of litigation following a breach.

The court's reference to "different scopes of work" among potential means of producing and protecting work product may signal a more viable option for companies considering how best to structure their arrangements with external advisers on cyber incident response. Potential strategies include:

- For those companies with a pre-existing relationship with a cybersecurity firm, requiring that external counsel enter into a new, different, and specific statement of work with the cybersecurity firm at the time of the breach;
- In connection with any breach, determining whether a report is necessary, and if so, the form of any deliverable;
- If an incident report is essential, implementing processes and procedures that will help limit its dissemination outside the legal department; and
- Being mindful of how payment of incident response services internally may be scrutinized by a court in considering whether any report prepared as part of those services was prepared for the purposes of litigation.

Employing these strategies may support a company's assertion that work product created by a cybersecurity consultant in response to a breach should be treated as protected work product if facing a court skeptical of that claim.

* * *

ENDNOTES

1 *See* Fed. R. Civ. P. 26(b)(3)(A) ("ordinarily, a party may not discover documents and tangible things that are prepared in anticipation of litigation or for trial by or for another party or its representative (including the other party's attorney, consultant, surety, indemnitor, insurer, or agent")); Fed. R. Evid. 502(g)(2) ("work-product protection" means the protection that applicable law provides for tangible material (or its intangible equivalent) prepared in anticipation of litigation or for trial").

2 *See* Information on the Capital One Cyber Incident (Sept. 23, 2019), https://www.capitalone.com/facts2019/.

3 *Id.*

4 Memorandum Order and Opinion, *In re: Capital One Customer Data Sec. Breach Litig.*, No. 1:19-MD-02915, Doc. No. 641 at 2 (E.D. Va. June 25, 2020) ("Trenga Opinion").

5 *Id.* at 2-3.

6 *See* Transfer Order, *In re: Capital One Customer Data Sec. Breach Litig.*, No. 1:19-MD-02915, Doc. No. 1 (J.P.M.L. Oct. 2, 2019).

7 Trenga Opinion at 3.

8 *In re: Capital One Customer Data Sec. Breach Litig.*, 2020 WL 2731238, at *4 (E.D. Va. May 26, 2020) ("Magistrate Opinion").

9 Magistrate Opinion at *3, citing *Nat'l Union Fire Ins. Co. of Pittsburgh, Pa.* v. *Murray Sheet Metal Co.*, 967 F.2d 980, 984 (4th Cir. 1992); *RLI Insurance Co.* v. *Conseco, Inc.*, 477 F. Supp. 2d 741, 747 (E.D. Va. 2007).

10 Magistrate Opinion at *4.

11 *RLI Insurance Co.*, 477 F. Supp. 2d at 747.

12 "More to the point, the Order incentivizes companies to either (a) forego keeping an incident response vendor on retainer or (b) hire a new, unfamiliar vendor to investigate any incident from which litigation is expected to result. But that is unworkable. . . . If courts preclude companies from asserting work product protection over materials prepared by a vendor with whom they have a pre-existing relationship, then companies will be less likely to plan ahead in engaging capable service providers, and may even avoid using the best service provider for a given need, as doing so would place the work product at risk of disclosure." Supporting Brief, Capital One Rule 72 Objections, *In re: Capital One Customer Data Sec. Breach Litig.*, No. 1:19-MD-02915, Doc. No. 557 at 20 (June 9, 2020).

13 *Id.* at 16.

14 Trenga Opinion at 9.

15 *Id.* at 2-3.

16 *Id.* at 12.

17 *Id.* at 13.

18 *Id.* at 13, n.8.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers listed below, or to any other Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.

CONTACTS

New York		
H. Rodgin Cohen	+1-212-558-3534	cohenhr@sullcrom.com
Mitchell S. Eitel	+1-212-558-4960	eitelm@sullcrom.com
John Evangelakos	+1-212-558-4260	evangelakosj@sullcrom.com
Jared M. Fishman	+1-212-558-1689	fishmanj@sullcrom.com
Nicole Friedlander	+1-212-558-4332	friedlandern@sullcrom.com
Scott D. Miller	+1-212-558-3109	millersc@sullcrom.com
Sharon L. Nelles	+1-212-558-4976	nelless@sullcrom.com
Matthew A. Schwartz	+1-212-558-4197	schwartzmatthew@sullcrom.com
Alexander J. Willscher	+1-212-558-4104	willschera@sullcrom.com
Michael M. Wiseman	+1-212-558-3846	wisemanm@sullcrom.com
Washington, D.C.		
Julia M. Jordan	+1-202-956-7535	jordanjm@sullcrom.com
Kamil R. Shields	+1-202-956-7040	shieldsk@sullcrom.com
Los Angeles		
Anthony J. Lewis	+1-310-712-6615	lewisan@sullcrom.com
Robert A. Sacks	+1-310-712-6640	sacksr@sullcrom.com
Palo Alto		
Nader A. Mousavi	+1-650-461-5660	mousavin@sullcrom.com
Sarah P. Payne	+1-650-461-5669	paynesa@sullcrom.com