IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

IN RE: CAPITAL ONE CONSUMER DATA SECURITY BREACH LITIGATION	)	MDL No. 1:19md2915 (AJT/JFA)

This Document Relates to the Consumer Cases

MEMORANDUM OPINION AND ORDER

This matter is before the court on plaintiffs' motion to compel production of Mandiant Report and related materials. (Docket no. 412). Plaintiffs have filed a memorandum in support (Docket nos. 413, 416), Capital One has filed an opposition (Docket no. 435), and plaintiffs have filed a reply (Docket nos. 445, 447). The court heard argument on this motion on May 15, 2020. Having reviewed the pleadings filed by the parties and considered the arguments raised by counsel, and for the reasons stated below, the court finds that Capital One has not carried its burden of establishing that the Mandiant Report is entitled to protection under the work product doctrine.

Background

Capital One entered into a Master Services Agreement ("MSA") with FireEye, Inc., d/b/a Mandiant ("Mandiant") on November 30, 2015, and thereafter entered into periodic Statements of Work ("SOW") and purchase orders with Mandiant pursuant to the MSA. (Blevins Decl. ¶ 4, Docket no. 435-1). As stated by Jeffrey Blevins II, a senior manager of Capital One's Cyber Security Operations Center, "one purpose of the MSA and associated SOWs was to ensure that Capital One could quickly respond to a cybersecurity incident should one occur. As a financial institution that stores financial and other sensitive information, it is critical that Capital One be

positioned to immediately respond to any potential compromise of the security of its systems." (*Id.* at ¶ 5). The SOWs with Mandiant provided for incident response services in the event such services were necessary. (*Id.* at ¶ 6). Capital One paid Mandiant a retainer for the SOW that was executed with Mandiant on January 7, 2019, and it entitled Capital One to 285 hours of services from Mandiant. (*Id.* at ¶ 8). In February 2019 Capital One designated the retainer paid to Mandiant as a "Business Critical" expense and not a "Legal" expense. (Docket no. 416-3 at 13, Docket no. 435 at 18). The SOW between Capital One and Mandiant in 2019 provided that Mandiant would provide incident response services during the covered period in the following areas: computer security incident response support; digital forensics, log, and malware analysis support; and incident remediation assistance and that Mandiant would provide a detailed final report covering the engagement activities, results and recommendations for remediation in a written detailed technical document. (Docket no. 416-2 at 3–4).

As described in detail in the Corrected Representative Consumer Class Action Complaint (Docket no. 354), in March 2019 a data breach occurred whereby an unauthorized person gained access to certain types of personal information relating to Capital One customers. In its opposition, Capital One states that on July 19, 2019, it confirmed that a data breach had occurred. (Docket no. 435 at 6). On July 20, 2019, Capital One retained Debevoise & Plimpton ("Debevoise") to provide legal advice in connection with the data breach incident. (Cantwell Decl. ¶ 3, Docket no. 435-2). 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." (Docket no. 435-2 at 6–8).[1] The Letter Agreement provides that the payment

[1] The description of services in the Letter Agreement are the same as those set forth in the SOW dated January 7, 2019, between Capital One and Mandiant. (Docket no. 416-2 at 3).

terms were to be the same as those set out in the SOW dated January 7, 2019, between Capital One and Mandiant and the parties would abide by the applicable terms in the SOW and MSA between Capital One and Mandiant dated November 30, 2015. (*Id.*). While the Letter Agreement provides for the same services to be performed by Mandiant under the same terms as the SOW and MSA, the Letter Agreement provides that the work would be done at the direction of counsel and the deliverables would be provided to counsel instead of Capital One. (*Id.*). On July 26, 2019, an addendum to the Letter Agreement was prepared whereby the engagement of services would also include penetration testing of systems and endpoints. (*Id.* at 10).

On July 29, 2019, Capital One issued a public announcement concerning the data breach. (Cantwell Decl. ¶ 3). The following day the first of many lawsuits was filed against Capital One asserting claims based on the data breach. *See Baird v. Capital One Fin. Servs. Corp.*, No. 1:19cv979 (LMB/JFA) (E.D. Va. filed July 30, 2019). 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." (Cantwell Decl. ¶ 19). The Mandiant Report was issued on September 4, 2019. (Docket no. 435 at 10). Mandiant was paid for its initial work under the Letter Agreement out of the retainer already provided to Mandiant under the January 7, 2019 SOW between Mandiant and Capital One. (Watts Decl. ¶ 3, Docket no. 435-3). After the retainer amount was exhausted, Mandiant's additional fees were paid directly by Capital One through the budget for the Cyber organization. (*Id.* ¶ 4). In December 2019 the expenses associated with the work Mandiant performed relating to the data breach were re-designated as legal expenses and deducted against Capital One's legal department's budget. (*Id.* at ¶ 5).

In addition to Mandiant, an internal investigation into the data breach was instituted involving a manager from Capital One's cyber incident management team and the Chief Information Security Officer that was separate from, and proceeded parallel to, Mandiant's investigation. (Blevins Decl. ¶ 16). Capital One has identified certain internal and external investigations that were undertaken in response to the data breach incident in its answer to plaintiffs' interrogatory number 11 (Docket no. 416-13 at 22–23) indicating that it does not "categorically claim work product protection or privilege over all of these company-led investigations" and "will produce documents relating to certain of them" (Docket no. 435 at 16). The brief summary of the work conducted and description of the results of the internal investigations set forth in the response to interrogatory number 11 is not sufficient for the court to determine the full nature and extent of those investigations and how the results were used within Capital One. Furthermore, Capital One has provided no detail concerning which of these internal investigations it will be producing documents for and the extent of its document production concerning those internal investigations.

The Mandiant Report was initially sent to Debovoise, which in turn provided the report to "Capital One's legal department." (Cantwell Decl. ¶ 20). Debovoise also provided the Mandiant Report to Capital One's Board of Directors. (*Id.* at ¶ 22). Exhibit 2 to Capital One's opposition states that it contains "a list of those to whom the Mandiant report was disclosed." (Docket no. 435-5). This list includes 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 (Ernest & Young). (*Id.*). There is no explanation provided as to why each recipient was provided with a copy of the Mandiant Report and whether the disclosure was related to a business purpose or for the

purposes of litigation. Even for those within the legal department, it is unclear if they were provided with the Mandiant Report in relation to duties involving the litigation or for regulatory or other business reasons. While the Cantwell declaration states the Mandiant Report was distributed to Capital One's Board of Directors, the list provided by Capital One's counsel does not appear to include those individuals. While there is an item named "corporate governance office general email box" on the list, there is no indication who has access to that "general email box." Capital One's opposition also fails to address what, if any, restrictions were placed on those persons and entities who received a copy of the Mandiant Report on discussing, copying, or providing the Mandiant Report, or any portion of it, to others.

As described in the Cantwell declaration, during Mandiant's investigation, it had communications with Ernst & Young, Capital One's outside auditor, related to Mandiant's confirmation of certain facts so that Ernst & Young was able to conclude that the data breach had no impact on Capital One's internal controls over financial accounting. (Cantwell Decl. ¶¶ 13, 14, *see also* Docket no. 416-6). It also appears that individuals within Capital One anticipated using the Mandiant Report in making certain disclosures required under the Sarbanes Oxley Act (Docket no. 416-4) and that the Mandiant Report was provided to an employee "for 2nd line business need" (Docket no. 416-11).

Legal Standards

In large part the parties agree on the legal principles involved. First, there is no dispute that Capital One, the party asserting work product doctrine, bears the burden of demonstrating the applicability of that doctrine. *Solis v. Food Employers Labor Relations Ass'n*, 644 F.3d 221, 232 (4th Cir. 2011); *Sandberg v. Virginia Bankshares, Inc.*, 979 F.2d 332, 355 (4th Cir. 1992). Also, it is well-established that courts generally disfavor assertions of evidentiary privileges

because they shield evidence from the truth-seeking process; as such, they are to be narrowly and strictly construed so that they are confined to the narrowest possible limits consistent with the logic of its principle. *In re Grand Jury Proceedings*, 727 F.2d 1352, 1355 (4th Cir. 1984), *RLI Ins. Co. v. Conseco, Inc.*, 477 F. Supp. 2d 741, 748 (E.D. Va. 2007).

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). As the Fourth Circuit discussed in *National Union Fire Ins. Co. v. Murray Sheet Metal Co.*, 967 F.2d 980, 984 (4th Cir. 1992), the fact that there is litigation does not, by itself, cloak materials with work product immunity but 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. *Id.* 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. *Id.*

In *RLI*, Judge Payne thoroughly discussed the *National Union* decision and interpreted the "because of" standard in that decision. *RLI*, 477 F. Supp. 2d at 746–49. 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. *Id.* at 747. The work product doctrine withholds protection from documents that would have been created in essentially similar form irrespective of the litigation. *Id.* Accordingly, 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.[2] *Id.* at 748.

Analysis

There is 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. Therefore, the determinative issue is whether the Mandiant Report would have been prepared in substantially similar form but for the prospect of that litigation.

As recognized in *RLI*, the party requesting protection under the work product doctrine bears the burden of showing how it would have investigated the incident differently if there was no potential for litigation. *RLI*, 477 Supp. 2d at 749–50. The hiring of outside counsel does not excuse a company from conducting its duties and addressing the issues at hand. *Id.* 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. For the reasons discussed below, Capital One has not presented sufficient evidence to show that the incident response services performed by Mandiant would not have been done in substantially similar form even if there was no prospect of litigation.

Capital One had a long-standing relationship with Mandiant and had a pre-existing SOW with Mandiant to perform essentially the same services that were performed in preparing the subject report. The services to be provided in the January 7, 2019 SOW are the same services

[2] Given the ruling on the work product issue based on the "because of" standard, it is not necessary to address the waiver or substantial need issues discussed by the parties in their briefs. That said, it appears that the waiver argument may have some merit given the lack of evidence presented in this motion concerning the distribution of the Mandiant Report and what protections were taken to avoid having the Mandiant Report or the information contained therein disclosed to a person or entity in an adversarial relationship. As to substantial need, while it would be more efficient for the plaintiffs to have the results of Mandiant's investigation, based on current record it appears that the event logs and network diagrams reviewed by Mandiant may be available to the plaintiffs.

described in the Letter Agreement. Capital One's senior manager of the cyber security operations center and the person responsible for managing Capital One's relationship with Mandiant acknowledged that as a financial institution that stores sensitive financial and other sensitive information, it is critical that it be positioned to immediately respond to any potential compromise of the security of its systems. (Blevins Decl. ¶ 5). The retainer paid to Mandiant was considered a business-critical expense and not a legal expense at the time it was paid. While the fact that the Mandiant Report was provided to four different regulators and to Capital One's accountant may not necessarily constitute a waiver, it does show that the results of an independent investigation into the cause and the extent of the data breach was significant for regulatory and business reasons. This independent investigation was also 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 data breach. (Docket no. 436-12).[3] The only significant evidence that Capital One has presented concerning the work Mandiant performed is that the work was at the direction of outside counsel and that the final report was initially delivered to outside counsel. Capital One's outside counsel states that Mandiant issued a written report detailing the technical factors that allowed the criminal hacker to penetrate Capital One's security. There is no statement by Capital One, or evidence upon which one could find, that Capital One would not have called upon Mandiant to perform the services described in the SOW that existed prior to the data breach and prepare a written report as provided in the SOW that would have detailed the results of its investigation, including detailing the technical factors that allowed the criminal hacker to penetrate Capital One's security.

[3] Capital One refers to these as "investor relations 'talking points'" in its opposition and argues that plaintiffs have offered no evidence showing these talking points were ever used. (Docket no. 435 at 18). However, Capital One has not provided any evidence that the talking points were not used.

Capital One has cited several cases in support of its argument that the Mandiant Report is protected work product including *In re Experian Data Breach Litig.*, 2017 WL 4325583 (C.D. Cal. May 18, 2017); *In re Arby's Rest. Grp., Inc. Data Sec. Litig.*, No. 1:17mi55555-WMR (N.D. Ga. March 25, 2019) Doc. No. 453; *In re Target Corp. Customer Data Sec. Breach Litig.*, 2015 WL 6777384 (D. Minn. Oct. 23, 2015); and *Genesco, Inc. v. Visa, Inc.*, No. 3:13-cv-00202 (M.D. Tenn. Mar. 25, 2015), Doc. No. 969, at 2.

In *Experian*, the court applied the same test as applied by Judge Payne in *RLI* and followed in this decision – that is, considering the totality of the circumstances can it 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 that litigation. *Experian*, 2017 WL 4325583 at *1. In finding that the report was protected as work product, the court noted that Experian immediately retained outside counsel and that outside counsel hired Mandiant to prepare a report. The court emphasized the timing of the retention of Mandiant by outside counsel and the fact the full report was not given to Experian's incident response team. The court stated that if the report "was more relevant to Experian's internal investigation or remediation effort, as opposed to being relevant to defense of the litigation, then the full report would have been given to that team." *Id.* at *3. The court then concluded that the report would not have been prepared in substantially the same form or with the same content. *Id.* One significant difference between the facts in *Experian* and the facts in this case is that Capital One had an *existing* SOW and MSA with Mandiant at the time of the data breach that was effectively transferred to outside counsel. As set out in the SOW and Letter Agreement, the work to be performed by Mandiant was the same, the terms were the same, but the work was to be performed at the direction of outside counsel and the final report delivered to outside counsel.

The retention of outside counsel does not, by itself, turn a document into work product. While it is true that in *Experian* the report was not given to Experian's response team, it appears that at least several members of Capital One's cyber technical, enterprise services, information security and cyber teams were provided with a copy of the Mandiant Report, and that it was used by Capital One for various business and regulatory purposes. As each case must be determined on its own facts and circumstances, the court cannot come to the same conclusion as the court in *Experian* that the work performed by Mandiant would not have been done in substantially the same form or with the same content.

The order in *Arby's* does not address in detail the facts underlying the ruling or the legal analysis for the conclusion that Arby's hired Mandiant to produce a report in anticipation of litigation and for other legal reasons and it is protected as work product and a privileged attorney-client communication. *Arby's*, No. 1:17mi55555-WMR (Docket no. 445-3). Accordingly, the court can divine no guidance from this decision.

In *Target*, the court also issued a brief order announcing its decision in which it provided very little factual background and no legal analysis on the work product issue. *Target*, 2015 WL 6777384. In essence this order merely announces a ruling on several challenged documents following an *in camera* review by the court and provides no assistance in resolving this case.

As in *Arby's* and *Target*, the order entered in *Genesco* referring to reasons stated in open court for its rulings provides no substantive guidance on the issues involved in this case. *Genesco*, No. 3:13-cv-00202 (Docket no. 445-2).

Plaintiffs have provided the court with two data breach cases that the court finds persuasive, one from the District of Oregon and one from this court. The decision in *Premera*, contains a discussion of the work product doctrine and how one should consider the application

of that doctrine when materials are prepared for "dual purposes." *In re Premera Blue Cross Customer Data Sec. Litig.*, 296 F. Supp. 3d 1230 (D. Or. 2017). The *Premera* court indicated that courts must view the totality of the circumstances and determine whether the document would have been created in substantially similar form but for the prospect of litigation. In discussing the Mandiant Remediation Report, the court noted that Mandiant was performing work for Premera and discovered the existence of malware in Premera's system. Premera then hired outside counsel and entered into an amended statement of work that shifted supervision of Mandiant's work to outside counsel. The amended statement of work did not otherwise change the scope of Mandiant's work from what was described in the master services agreement. The court distinguished the decision in *Target* on the basis that there was an independent data breach investigation performed by the company "that was produced in discovery" and that the attorneys performed a separate investigation through a retained expert company. The decision in *Experian* was distinguished because outside counsel hired Mandiant and in *Premera*, Mandiant had already been hired and was performing services for Premera before outside counsel became involved. The court also recognized that Premera had the burden of showing Mandiant changed the nature of its investigation at the instruction of outside counsel and that Mandiant's scope of work and purpose became different when outside counsel became involved.

Capital One attempts to distinguish this decision on the basis that at the time of the data breach Mandiant was not performing an *ongoing* investigation. While it is true that there was no ongoing investigation at the time of the data breach or its subsequent discovery, the court finds the fact that there was an existing SOW with a paid retainer that obligated Mandiant to perform 285 hours of service for Capital One in 2019, at the time of the data breach and its discovery, to be significant. Again, Capital One has not carried its burden of showing that Mandiant's scope

of work under the Letter Agreement with outside counsel was any different than the scope of work for incident response services set forth in the existing SOW and that it would not have been performed without the prospect of litigation.

Finally, the court also finds the *Dominion Dental* decision from this court to be particularly helpful. *In re Dominion Dental Servs. USA, Inc. Data Breach Litig.*, 2019 WL 7592343 (E.D. Va. Dec. 19, 2019). In that decision the court found that the defendants had failed to show that the Mandiant report would not have been completed in substantially similar form but for the prospect of litigation and granted the motion to compel. *Id.* at *5. In *Dominion Dental* the defendants argued that the Mandiant report "was created to inform legal counsel and litigation strategy" and was therefore protected work product. *Id.* at *1. Dominion Dental had hired Mandiant prior to the data breach involved in that case to investigate, prevent, and remediate data breaches. *Id.* At the time of the data breach, Dominion Dental and its outside counsel had a statement of work with Mandiant whereby Mandiant was to provide incident response services including "computer incident response support, digital forensics support, advanced threat actor support, and advanced threat/incident assistance." *Id.* After the data breach was discovered, Dominion Dental's outside counsel then entered into another statement of work with Mandiant incorporating the previous statement of work and master services agreement and including virtually the same deliverables as the statement of work that was in existence prior to the data breach. *Id.* at *2. *Dominion Dental* noted a reference in a list of talking points to retaining Mandiant, a world leading cyber security firm, to investigate the incident and that the Mandiant report appears to have been used with Dominion Dental's regulators. *Id.* The court discussed the same decisions cited by the parties in this case, *Experian* and *Target* relied upon by Capital One and *Premera* relied upon by the plaintiffs. *Id.* at *3.

Even in the face of a statement in an affidavit from Dominion Dental that the Mandiant report would not have been prepared in a substantially similar form and may not have been necessary at all without the threat of litigation, the court found Dominion Dental had not carried its burden, relying heavily upon the fact that the description of services in the statement of work in existence prior to the data breach was "almost identical" to the services in the post-data breach statement of work. *Id.* at *4. The fact that the post-data breach statement of work indicated that the work was to be "under the direction of Counsel" did not alter the business purposes of the work to be performed and appeared to be designed to help shield the report from disclosure. *Id.*

Capital One's attempts to distinguish the *Dominion Dental* decision are unpersuasive. First, Capital One has not shown that the *nature of the work* Mandiant had agreed to perform changed when outside counsel was retained. As discussed in detail above, and as was the case in *Dominion Dental*, the statement of works and master services agreements provided for virtually identical services to be performed before and after the data breaches were discovered. The fact that Dominion Dental waited two months to make a public announcement after it learned of the intrusion, at which time Mandiant had concluded its report, does not alter the legal analysis. Just as Capital One has argued here, that there "is no question that the Cyber Incident was the type of event that Capital One knew would lead to litigation" (Docket no. 435 at 12), there can be no question that Dominion Dental knew there was a prospect of litigation once the data breach had been discovered. Finally, Capital One argues that "there was no evidence" in *Dominion Dental* that the fruits of Mandiant's work were used for legal purposes. However, the record in *Dominion Dental* included an affidavit that the Mandiant report would not have been prepared in substantially similar form without the threat of litigation and that the statement of work was

modified to provide that the work was to be performed under the direction of counsel and if requested by counsel.

For these reasons, it is hereby

ORDERED that plaintiffs' motion to compel is granted in part. Capital One shall provide plaintiffs with a copy of the Mandiant Report pursuant to the terms of the Protective Order entered in this action. In accordance with Local Civil Rule 37(C), Capital One shall have eleven days to comply with this order. The plaintiffs' motion to compel "related materials" is denied without prejudice. As discussed in Capital One's opposition, the issues concerning all related materials is not ripe for decision. (Docket no. 435 at 28–30). The parties have not had an opportunity to discuss the claim of privilege over related materials and to consider any arguments that certain related materials may be entitled to be withheld from production even if the Mandiant Report was found not to be entitled to work product protection.

Entered this 26th day of May, 2020.

/s/
John F. Anderson
United States Magistrate Judge

Alexandria, Virginia

John F. Anderson
United States Magistrate Judge