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 CONSUMER Cases

CAPITAL ONE'S RULE 72 OBJECTIONS TO ORDER GRANTING PLAINTIFFS' MOTION TO COMPEL PRODUCTION OF MANDIANT REPORT

KING & SPALDING LLP

David L. Balser (*pro hac vice*)
S. Stewart Haskins II (*pro hac vice*)
John C. Toro (*pro hac vice*)
Kevin J. O'Brien (VSB No. 78886)
Robert D. Griest (*pro hac vice*)
1180 Peachtree Street, N.E.
Atlanta, Georgia 30309
Telephone: (404) 572-4600
Facsimile: (404) 572-5140
dbalser@kslaw.com
shaskins@kslaw.com
jtoro@kslaw.com
kobrien@kslaw.com
rgriest@kslaw.com

TROUTMAN SANDERS LLP

Robert A. Angle (VSB No. 37691)
Tim St. George (VSB No. 77349)
Jon S. Hubbard (VSB No. 71089)
Harrison Scott Kelly (VSB No. 80546)
1001 Haxall Point
Richmond, VA 23219
Telephone: (804) 697-1200
Facsimile: (804) 697-1339
robert.angle@troutman.com
timothy.st.george@troutman.com
jon.hubbard@troutman.com
scott.kelly@troutman.com

Mary C. Zinsner (VSB No. 31397)
401 9th Street, NW, Suite 1000
Washington, DC 20004
Telephone: (703) 734-4334
Facsimile: (703) 734-4340
mary.zinsner@troutman.com

Counsel for Capital One

TABLE OF CONTENTS

INTRODUCTION

Under Federal Rule of Civil Procedure 72(a) and 28 U.SC. § 636(b)(1)(A), Capital One respectfully asks this Court to set aside the Magistrate Judge's order compelling Capital One to produce the Mandiant Report to Plaintiffs (the "Order") (Dkt. 490). The Mandiant Report was prepared by cybersecurity consulting firm Mandiant, and there is no dispute that Mandiant was hired by, acted at the direction of, and reported solely to Debevoise & Plimpton LLP ("Debevoise"), Capital One's outside counsel. Nor can it be disputed that the Mandiant Report was prepared in anticipation of litigation. Even though the Mandiant Report bears all the hallmarks of protected work product, the Magistrate Judge concluded that it was not protected. That ruling should be set aside.

First, the Magistrate Judge ruled that because Capital One had a pre-existing contract with Mandiant for incident response services, Capital One had failed to prove the negative that the Mandiant Report would *not* have been prepared in the same form absent litigation. Capital One respectfully submits that the Magistrate Judge misapplied controlling law in reaching this conclusion. Put simply, there was no reason for the Court to engage in a hypothetical inquiry about the form the Mandiant Report might have taken absent litigation, in light of the *undisputed evidence* that (1) Capital One hired Debevoise to advise it with respect to anticipated litigation arising out of the data breach Capital One announced on July 29, 2019 (the "Cyber Incident"); (2) Debevoise hired Mandiant—under a separate engagement letter—to assist *it* in providing legal advice concerning that anticipated litigation; (3) Mandiant performed no investigative services relating to the Cyber Incident until after being retained by Debevoise; (4) Mandiant took direction from and reported solely to Debevoise; and (5) the Mandiant Report reflects the combined work product of Debevoise and Mandiant. From these *undisputed facts*, it is abundantly clear that the driving force behind the preparation of the Mandiant Report was to help Debevoise advise the

Company about the waves of litigation that began rolling in within 24 hours of Capital One's announcing the Cyber Incident (and weeks before the Mandiant Report was completed). Accordingly, it was clearly erroneous and contrary to law to conclude that the Mandiant Report is not protected work product.

In addition to being unnecessary, the Magistrate Judge's conclusion that the Mandiant Report would not have been meaningfully different absent litigation disregards several practical realities. Had there been no prospect of litigation, Mandiant would have worked with Capital One's Cyber organization employees (rather than legal counsel), and Mandiant's report would not reflect outside counsel's direction and input like the Mandiant Report does here. Moreover, the Order overlooks that Debevoise's engagement letter with Mandiant superseded the prior Capital One engagement letter, imposed different investigatory objectives, and directed Mandiant to report exclusively to Debevoise. Consequently, it was incorrect for the Magistrate Judge to conclude that the Mandiant Report would not have been prepared in substantially similar form without the prospect of litigation.

Second, the Magistrate Judge erred in relying on the fact that Capital One used the Mandiant Report for certain business-related purposes *after* it was created and used for its intended litigation purpose. Courts have long recognized that documents prepared in anticipation of litigation do not lose their work product protection just because they are later used for business purposes.

Accordingly, because the Mandiant Report is protected work product—and because there is no valid alternative basis to uphold the Magistrate Judge's Order, the Order should be set aside.

FACTUAL BACKGROUND

A. Mandiant's Work for Capital One Before the Cyber Incident

On November 30, 2015, Capital One and Mandiant entered into a Master Services Agreement ("MSA") under which Mandiant agreed to provide services to Capital One as specified in related Statements of Work ("SOW"). Motion to Compel Production of Mandiant Report and Related Materials ("Mot."), Ex. 1, Master Services Agreement (executed Nov. 24, 2015) (Dkt. 416-1, filed under seal), at -258941. Beginning in 2015, Capital One and Mandiant executed periodic SOWs for incident response services that might be needed during a given year. Mot. Ex. 2, Statement of Work (executed Jan. 7, 2019) (Dkt. 416-2, filed under seal), at -97223; Declaration of Jeffrey Blevins II (Dkt. 435-1) ¶ 4.[1] The purpose of these SOWs was to ensure that Mandiant would be on call and able to promptly assist Capital One in the event of a cybersecurity incident. *Id.* ¶ 5; *see also* Declaration of D.J. Palombo ¶ 9.[2] In fact, federal regulations *require* Capital One to have a plan in place for promptly responding to cybersecurity incidents.[3] *See*

---

[1] Capital One has not re-filed the declarations and exhibits attached to its original Opposition to the Plaintiffs' Motion to Compel Production of Mandiant Report and Related Materials (the "Opposition" or "Opp.") (Dkt. 435) and instead refers to those exhibits by docket number and, subsequently, by short form citation.

[2] Capital One submits the Declarations of D.J. Palombo and Heather Caputo for the first time with its Rule 72 Objections to clarify issues raised in the Magistrate Judge's order. *See Harleysville Ins. Co. v. Holding Funeral Home, Inc.*, No. 1:15-cv-00057, 2017 WL 2210520, at *2 (W.D. Va. May 19, 2017) (noting that it is within the district judge's "discretion to receive and consider additional evidence" when reviewing a magistrate judge's decision under Rule 72(a)); S*ky Angel U.S., LLC v. Discovery Commc'ns, LLC*, 28 F. Supp. 3d 465, 479 (D. Md. 2014) (same).

[3] That Capital One is required by regulation to have a plan in place for cybersecurity incident response explains why retainers Capital One paid to Mandiant *before* the Cyber Incident occurred were classified in company files as "business critical" expenses rather than "legal" expenses. *See* Order at 2; Opp. at 17; Mot. Ex. 3, Cyber Monthly Financial Review (Feb. 22, 2019) (Dkt. 416-3, filed under seal), at -185319; *see also* Declaration of Heather Caputo ¶ 5 (explaining that retainers paid prior to the Cyber Incident were for the "business critical" purpose of ensuring that Capital One complied with governing regulations and that the sums paid for Mandiant's work done for Debevoise were drawn from the legal budget).

generally 12 C.F.R. part 570, app. B, Interagency Guidelines Establishing Information Security Standards.

Under each SOW, Capital One paid Mandiant a retainer for up to 285 hours of incident response services. *See* Mot. Ex. 2 at -97224, -97225; Blevins Decl. ¶ 8. The SOWs were for Mandiant's "Incident Response *Retainer Service*" only. *See*, *e.g.,* Mot. Ex. 2 at -97223 (emphasis added). As such, the SOWs broadly outline the general type of incident response services Mandiant *might* provide to Capital One *if* Capital One and Mandiant decide it is necessary for Mandiant to perform services related to an incident. Palombo Decl. ¶ 10; *see also* Mot. Ex. 2 at -97223 ("*Upon engagement* for Incident Response Services . . . , the IR Lead will determine the appropriate next steps with [Capital One]." (emphasis added)). Since there are several different types of "incidents"[4] that might require Mandiant's services, the SOWs were intentionally drafted broadly, with the specifics of a particular engagement to be determined on a case-by-case basis after Capital One decided to engage Mandiant for an incident. *See* Palombo Decl. ¶ 10.

In the two years before the Cyber Incident, Capital One did not need Mandiant to provide any incident response services. Blevins Decl. ¶ 7. Instead of wasting the retainer paid to Mandiant for those years, Capital One and Mandiant agreed that the retainer would be used for Mandiant to perform other services, such as training and consulting work. *Id.* ¶ 9. So, when it became clear in 2018 that Mandiant's retainer fee would not be needed for incident response services, Capital One

[4] A security incident is a violation of a company's security policies that puts sensitive data at risk. *See, e.g.*, *Incident Definition*, Cybersecurity and Infrastructure Security Agency, https://www.us-cert.gov/government-users/compliance-and-reporting/incident-definition. It is a broad term that encompasses many different kinds of events, not all of which are data breaches. For example, a security incident could involve unregulated but sensitive data such as intellectual property or could involve a phishing scheme targeting a single employee (such as the CEO). That cybersecurity incidents can take many forms means that not every incident to which Mandiant might respond would necessarily result in litigation, involve the retention of counsel, or require the preparation of a formal report.

asked Mandiant to conduct a review of Capital One's cybersecurity incident "preparedness." *See id.* ¶ 10. The review was designed to evaluate and suggest improvements to Capital One's policies and procedures for responding to potential cybersecurity incidents. *Id.*

In the early summer of 2019, it again appeared that Capital One would not need to use Mandiant's retainer for incident response services. *Id.* ¶ 11. Capital One and Mandiant thus began negotiating for similar consulting services that Mandiant would provide. *Id.* But this work was put on hold after Capital One discovered the Cyber Incident in July 2019. *Id.*

B. Debevoise's Direct Engagement of Mandiant Following the Cyber Incident

On July 19, 2019, Capital One confirmed that the Cyber Incident had occurred. The company immediately retained Debevoise on July 20, 2019 to provide legal advice to Capital One and its Board of Directors concerning the litigation and regulatory activity anticipated to result from the Cyber Incident and to conduct a privileged investigation into the circumstances that gave rise to the Cyber Incident. Declaration of Helen Cantwell (Dkt. 435-2) ¶¶ 3-5; Blevins Decl. ¶¶ 12, 14. Given the scope of the Cyber Incident, Capital One understood that litigation would follow its announcement of the breach. Cantwell Decl. ¶ 5. Capital One was proven correct, as class action complaints started pouring in less than 24 hours after Capital One announced the Cyber Incident. But despite having a retainer agreement with Mandiant, Capital One did *not* reach out to Mandiant to request any services after it learned of the breach. Caputo Decl. ¶ 4.

Instead, Debevoise directly engaged Mandiant to assist in its privileged investigation. Cantwell Decl. ¶ 6. Mandiant did not perform any work on the Cyber Incident before being engaged by Debevoise. *Id.*; Blevins Decl. ¶ 14; Palombo Decl. ¶ 15. And although Capital One had previously entered into a general MSA with Mandiant, Debevoise's direct engagement of Mandiant following the Cyber Incident set out the specific terms of the work Mandiant would perform at Debevoise's direction. *Compare* Cantwell Decl. Ex. A, Debevoise-Mandiant-Capital

One Engagement Letter, (Dkt. 435-2) at 6 (providing that Mandiant's work for Debevoise would be "as directed by [Debevoise]," that the "Services under th[e] Letter are done at [Debevoise's] request," and that "all Deliverables . . . shall be properly communicated to . . . [and] delivered to [Debevoise]," "notwithstanding any prior agreements between Mandiant and [Capital One].") *with* Mot. Ex. 2 at -97223, -97224 (requiring Mandiant to provide services and deliverables directly to Capital One).

Debevoise's selection of Mandiant was not automatic. Despite the prior agreement, neither Capital One nor Debevoise was under any obligation to hire Mandiant for the Cyber Incident, *see* Palombo Decl. ¶ 13, and Capital One and Debevoise deliberated about which cybersecurity firm was best suited to assist Debevoise, *see* Caputo Decl. ¶ 6. But the exigent circumstances—and the fact that Mandiant had already been onboarded, cleared to receive sensitive Capital One information, and could begin work immediately without the months of delay that would follow the selection of another firm—weighed in favor of hiring Mandiant. *Id.* ¶¶ 6, 10. Debevoise also engaged Mandiant because of "Mandiant's specific expertise and prior experience in investigating other major data breaches." Cantwell Decl. ¶ 7.

The agreement signed by Debevoise, Mandiant, and Capital One on July 24, 2019 confirmed Mandiant's specific role with respect to the Cyber Incident, making clear that Mandiant would provide assistance directly to Debevoise in connection with its privileged investigation and provision of legal advice to Capital One. *See* Cantwell Decl. Ex. A (Dkt. 435-2) at 6-7 (noting that Mandiant was retained to "provide services and advice, *as directed by* [Debevoise]" in numerous technical areas (emphasis added)). On July 26, 2019, Debevoise and Mandiant executed an addendum to that agreement, expanding the scope of Mandiant's services to include assessing the remediation of the technical vulnerability that gave rise to the Cyber Incident. Cantwell Decl.

Ex. B, Addendum to the Debevoise-Mandiant-Capital One Engagement Letter (Dkt. 435-2), at 10-11. In short, the work Mandiant was hired to perform for Debevoise was different from that called for under the 2019 SOW in terms of scope, timeframe, and deliverables. Caputo Decl. ¶ 12.

Less than a week after Debevoise retained Mandiant, the first class action lawsuit arising out of the Cyber Incident was filed against Capital One. *See* Dkt. 1, *Baird v. Capital One Fin. Corp.*, No. 1:19cv979 (LMB/JFA) (E.D. Va. filed July 30, 2019).

C. Mandiant's Work for Debevoise on the Cyber Incident

Mandiant played a critical role in Debevoise's investigation, assisting counsel in assessing and understanding technical aspects of the Cyber Incident. Cantwell Decl. ¶ 15; Cantwell Decl. Ex. A (Dkt. 435-2 at 6). Specifically, Mandiant assisted Debevoise by (1) helping Debevoise understand and interpret technical matters it encountered in its review of documents and witness interviews; (2) consulting on specific sub-investigations Debevoise conducted on technical matters; and (3) performing a "red team" exercise to assess the vulnerability that led to the Cyber Incident. Cantwell Decl. ¶ 16. Debevoise defined these specific objectives when it retained Mandiant. *See* Palombo Decl. ¶¶ 14-15. In all, the work Mandiant performed significantly enhanced Debevoise's ability to provide legal advice to Capital One. Cantwell Decl. ¶ 17.

Importantly, Mandiant's work for Debevoise was entirely distinct from the internal investigations that Capital One's Cyber Organization[5] conducted to understand the root causes of the Cyber Incident, develop a strategy for remediating those root causes, and chart a path forward for enhancing the company's overall cybersecurity program. *See* Mot. Ex. 13, Capital One Defendants' Amended Responses to Plaintiffs' First Interrogatories (Dkt. 416-13, filed under seal), at 21-23 (describing the various investigations Capital One pursued in response to the Cyber

[5] Capital One's Cyber Organization is the team at Capital One primarily responsible for cybersecurity and remediating the issues that led to the Cyber Incident.

Incident); Ex. 1, Dep. M. Fisk 36:24-37:4, 94:24-95:7 [redacted] For example, while Mandiant's work focused on analyzing the technical aspects of the Cyber Incident and did not include a root cause analysis, [redacted].

Although the work Mandiant performed was governed by the July 2019 Debevoise-Mandiant engagement—not the general retainer agreement between Mandiant and Capital One—the company's existing relationship with Mandiant did allow Debevoise to promptly engage Mandiant and bypass the administrative hurdles associated with onboarding a new third-party service provider. *See* Cantwell Decl. ¶¶ 9-10; Blevins Decl. ¶ 13. As a federally regulated bank that stores sensitive information, Capital One has a rigorous process for vetting third-party service providers before granting them access to its systems. Blevins Decl. ¶ 5; Caputo Decl. ¶¶ 7-8. Because Capital One had already vetted Mandiant as a reliable and secure service provider, Mandiant was able to promptly gain access to Capital One's systems to perform the work Debevoise hired it to do. *See* Blevins Decl. ¶¶ 5, 13; Cantwell Decl. ¶ 10; Caputo Decl. ¶ 10.

Like other vendors retained by Debevoise, Mandiant billed Capital One directly. Cantwell Decl. ¶ 11. Because the retainer Capital One paid to Mandiant for 2019 had not been exhausted, Mandiant was initially paid from it. Declaration of David Watts (Dkt. 435-3) ¶ 3. But once those funds were exhausted, Mandiant's additional payments were made from Capital One's legal

budget for expenditures relating to the Cyber Incident.[6] *Id.* ¶ 4. In all events, Capital One's payment arrangement with Mandiant did not affect Debevoise's complete supervision of Mandiant's work (*see id*. ¶ 4), and it is typical for clients to directly pay expert consultants for work performed for outside counsel (*see* Cantwell Decl. ¶ 11).

Debevoise directed and supervised all of Mandiant's work and communications on the Cyber Incident. *See* Opp. Ex. 1 (Dkt. 435-4) at 2 ("At this point since ***Cyber isn't directing [Mandiant's] work or resources***, can you please send these types of messages to [Capital One's in-house counsel] . . . ." (emphasis added)). So, when Mandiant had to communicate with certain Capital One employees—including during witness interviews that Debevoise attorneys led—it did so at Debevoise's direction. Blevins Decl. ¶ 17; Cantwell Decl. ¶ 18; Palombo Decl. ¶ 17. Moreover, Mandiant reported only to Debevoise, and did not share its analysis with Capital One employees. Blevins Decl. ¶ 18; Cantwell Decl. ¶ 20; Palombo Decl. ¶ 17.

Debevoise also directed Mandiant to communicate with Ernst & Young ("EY"), Capital One's auditor. Cantwell Decl. ¶ 13. These communications, which occurred roughly five weeks before Mandiant issued its final report to Debevoise, were limited to Mandiant's confirmation of discrete facts necessary for EY to conclude that the Cyber Incident had no impact on Capital One's financial systems or internal controls over financial reporting. *Id.* ¶ 14.

D. Mandiant Issues Its Investigative Report Directly to Debevoise

On September 4, 2019, Mandiant issued its Report to Debevoise. Palombo Decl. ¶ 16. The Report's content was driven by the investigatory objectives that Debevoise conveyed when it

[6] Though the additional funds paid to Mandiant were initially drawn from the Cyber Organization's budget, this was done for administrative efficiency only. Watts Decl. ¶ 4. All of the payments for the work Mandiant did for Debevoise were ultimately deducted from the company's *legal* budget after a routine year-end accounting reconciliation of the expenses incurred in connection with the Cyber Incident. *See id.* ¶ 5; *see also* Caputo Decl. ¶ 5.

engaged Mandiant, and Debevoise had input into the Report's format and content. *Id.* ¶¶ 6, 16. Had the Report been prepared primarily for business purposes, it would have likely taken a different form by, for example, providing recommendations for remediating the effects of the Cyber Incident instead of focusing on assessing the technical factors that led to the Incident. Caputo Decl. ¶ 12; *see also* Palombo Decl. ¶ 6 (noting that the involvement of counsel affects the content of the reports generated by Mandiant).

After it was delivered to Debevoise in its final form, the Mandiant Report was initially shared only with Capital One's legal team. Cantwell Decl. ¶ 20. Capital One's legal team later shared the Report only with select non-lawyer employees who had a specific need to examine it, and each of those recipients was tracked and logged. *See* Opp. Ex. 2 (Dkt. 435-5 at 8-9) (attaching a list of recipients of the Mandiant Report in response to Plaintiffs' supplemental discovery requests); Caputo Decl. ¶ 13. In a company that employs roughly 700 people in its Cyber Organization alone and thousands more in other information technology functions, only 31 non-legal Capital One employees and the Corporate Governance Office email box were ultimately given access to the Report.[7] *Id.* ¶¶ 12, 15. Only a handful of these recipients were members of the Cyber Organization itself. *Id.* ¶ 12. Many of these individuals were employed in accounting, risk management, and audit functions—all areas where Capital One has extensive regulatory and legal obligations which require advisory services. *Id.* ¶ 17. Many more were in the "control group" of senior managers working to address the effects of the Cyber Incident and to provide advice and counseling on Capital One's regulatory and legal obligations relating to the Cyber Incident. *Id.*

[7] Seven individuals had access to the Corporate Governance Office email box, only two of whom were non-legal staff. Caputo Decl. ¶ 18. All seven employees needed access to the Mandiant Report because their jobs involve "managing communications with and prepar[ing] . . . materials for the Board of Directors." *Id*.

¶ 16. As such, all of the Report's recipients had a critical need to know about the information in the Report. *Id.* ¶ 13. After delivering the Report to Capital One's legal team, Debevoise separately attached it to a report it provided to Capital One's Board of Directors at the conclusion of its investigation. Cantwell Decl. ¶ 22; Caputo Decl. ¶ 19.

Disclosure of the Report outside the company was even more limited. Capital One provided the Report in response to requests from four federal supervisory bank regulators—the OCC, the FRB, the FDIC, and the CFPB—and to its auditor, EY. Cantwell Decl. ¶ 21.

LEGAL STANDARDS

A. The Standard of Review

Under the Federal Rules of Civil Procedure, "[t]he district judge in the case must consider timely objections" to a magistrate judge's decision on "a pretrial matter not dispositive of a party's claim or defense" and must "modify or set aside any part of the order that is clearly erroneous or is contrary to law." Fed. R. Civ. P. 72(a); *see also* 28 U.S.C. § 636(b)(1)(A). An order is "clearly erroneous" where "the reviewing court on the entire evidence is left with the definite and firm conviction that a mistake has been committed." *United States v. U.S. Gypsum Co.*, 333 U.S. 364, 395 (1948). On the other hand, "[t]here is no practical difference between review under Rule 72(a)'s contrary to law standard and [a] de novo standard." *Bruce v. Hartford*, 21 F. Supp. 3d 590, 594 (E.D. Va. 2014) (citation omitted). "[A]n order is contrary to law 'when it fails to apply or misapplies relevant statutes, case law, or rules of procedures.'" *MeadWestvaco Corp. v. Rexam, PLC*, No. 1:10cv511 (GBL/TRJ), 2011 WL 2938456, at *2 (E.D. Va. July 18, 2011). That is, the Magistrate Judge's legal conclusions—and applications of law to fact—are entitled to no deference. *See id.*[8]

[8] A few cases from courts in this District have suggested that Rule 72(a)'s "contrary to law" standard is more deferential than plenary review if the order concerns a discovery dispute. *See,*

B. The Work Product Doctrine

The work product doctrine protects "documents and tangible things that are prepared in anticipation of litigation or for trial by or for [a] party or its representative." Fed. R. Civ. P. 26(b)(3). A document that is "prepared *because of* the prospect of litigation" qualifies for work product protection. *Nat'l Union Fire Ins. Co. of Pittsburgh v. Murray Sheet Metal Co.*, 967 F.2d 980, 984 (4th Cir. 1992). The determinative issue is the "driving force behind the preparation of [the] document." *Id.* A document prepared in the ordinary course of business thus is not work product even though it may also serve a litigation-related purpose. *Id.* But a document prepared because of litigation is still work product even though it might later be used for business reasons. *See, e.g.*, *United States v. Deloitte LLP*, 610 F.3d 129, 138 (D.C. Cir. 2010) ("Under the more lenient 'because of' test, material generated in anticipation of litigation may also be used for ordinary business purposes without losing its protected status.").

ARGUMENT

I. THE COURT SHOULD SET ASIDE THE MAGISTRATE JUDGE'S CONCLUSION THAT THE MANDIANT REPORT IS NOT PROTECTED WORK PRODUCT.

The Magistrate Judge misapplied the Fourth Circuit's "because of" standard. A document is entitled to work product protection when the prospect of litigation was the "driving force behind [its] preparation." *Nat'l Union*, 967 F.2d at 984. In determining whether that standard has been met, courts consider whether "the [party] faces an actual claim or a potential claim following an

---

e.g., *Malibu Media, LLC v. John Does 1–23*, 878 F. Supp. 2d 628, 629 (E.D. Va. 2012). But even if the "contrary to law" standard were as deferential as an abuse of discretion standard in those instances, a court "by definition abuses its discretion when it makes an error of law." *Koon v. United States*, 518 U.S. 81, 100 (1996); *see Cunningham v. Johnson*, 241 F. App'x 913, 917 (4th Cir. 2007) (similar). Thus, because the Magistrate Judge's conclusion that the Mandiant Report is not protected work product rests on a misapplication of applicable law, this Court should "set aside" that ruling as "contrary to law." Fed. R. Civ. P. 72(a).

actual event or series of events that reasonably could result in litigation," and also ask whether "the work product would not have been prepared in substantially similar form but for the prospect of that litigation." *RLI Ins. Co. v. Conseco, Inc.*, 477 F. Supp. 2d 741, 748 (E.D. Va. 2007) (quoting *Nat'l Union*, 967 F.2d at 984 and *United States v. Adlman*, 134 F.3d 1194, 1195 (2d Cir. 1998)). The Mandiant Report satisfies both prongs of this test, but the Magistrate Judge applied the test in an unduly restrictive manner to hold that the second prong was not satisfied. *See* Order at 7-10.

The Magistrate Judge's conclusion that Capital One had failed to show that the Mandiant Report would not have been prepared in substantially similar form absent litigation rests on two grounds: (1) that Capital One had a "pre-existing SOW with Mandiant to perform essentially the same services" that are "described in the Letter Agreement" with Debevoise, *id.* at 7, and (2) that the Mandiant Report was used for some "regulatory and business reasons" after its preparation, *id.* at 8. The Magistrate Judge erred by focusing on the nature of the work Mandiant *could have* done for Capital One under the pre-existing SOW—rather than the Report actually prepared by Mandiant under Debevoise's direction—and incorrectly held that the limited, business uses to which the Mandiant Report was put *after* its preparation stripped it of protection.

A. The Mandiant Report Was Prepared Because of the Prospect of Litigation Arising Out of the Cyber Incident.

1. Litigation was the driving force behind the Mandiant Report.

While there is no "hard and fast rule" to determine whether a document was prepared because of the prospect of litigation, courts in this circuit consider a range of factors, including (1) the nature of the documents, (2) the nature of the litigation, (3) the relationship between the parties, (4) other facts peculiar to the case, (5) the involvement of counsel, and (6) the time when the document is created. *Lewis v. Richland Cty. Recreation Comm'n*, No. 3:16-cv-2884 (MGL/TER), 2018 WL 4596119, at *6 (D.S.C. Sept. 25, 2018) (citing *Kidwiler v. Progressive Paloverde Ins.*

Co., 192 F.R.D. 536, 542 (N.D.W. Va. 2000)). Here, all of these factors show that litigation was the "driving force" behind the preparation of the Mandiant Report, and thus that it is protected work product.

Debevoise was hired to "help the company prepare for and defend against litigation" that Capital One anticipated would (and did) follow announcement of the Cyber Incident. Cantwell Decl. ¶ 5; *see also* Caputo Decl. ¶ 6. Debevoise in turn hired Mandiant, after considering numerous vendors, to provide forensic services to assist in Debevoise's investigation and its provision of legal advice to the company; the very purpose of the Mandiant Report—from the beginning—was to inform and facilitate Debevoise's investigation and advice. Caputo Decl. ¶ 6; Cantwell Decl. ¶¶ 6, 19. In keeping with that purpose, the Mandiant Report was incorporated into Debevoise's own final report about the Cyber Incident that was provided to the Board. *Id.* ¶ 22. Thus, the "driving force" behind the Mandiant Report was to assist Debevoise, and Debevoise would not have been hired but for the risk of litigation and regulatory activity attendant to the Cyber Incident. That conclusion alone warrants setting aside the Order.

To be sure, Capital One had a pre-existing contract with Mandiant and could have hired Mandiant directly to investigate a data breach for either litigation or business purposes. The pertinent question, though, is *which* purpose prompted Mandiant's retention for the Cyber Incident. And here, the undisputed evidence makes it clear that Mandiant was engaged to aid in the investigation Debevoise conducted to help the company prepare for litigation.

Underscoring this point, numerous courts have held reports like the Mandiant Report to be protected work product. *See, e.g.*, *In re Arby's Rest. Grp., Inc. Data Sec. Litig.*, No. 1:17-mi-55555-WMR (N.D. Ga. Mar. 25, 2019), Doc. No. 453 (denying motion to compel Mandiant report) (attached as Exhibit 3); *In re Experian Data Breach Litig.*, No. 15-01592 (DFMx), 2017 WL

4325583, at *2 (C.D. Cal. May 18, 2017) (same); *In re Target Corp. Customer Data Sec. Breach Litig.*, No. MDL 14-2522 (PAM/JJK), 2015 WL 6777384, at *3 (D. Minn. Oct. 23, 2015) (similar); *Genesco, Inc. v. Visa, Inc.*, No. 3:13-cv-00202 (M.D. Tenn. Mar. 25, 2015), Doc. No. 969, at 2 (similar) (attached as Exhibit 4).

The *Experian* decision involved facts similar to those present here. There, Experian retained Jones Day for legal advice following a data breach, and Jones Day in turn "hired Mandiant to conduct an expert … analysis of the attack" to "help [it] provide legal advice to Experian regarding the attack." 2017 WL 4325583, at *2. Although the Magistrate Judge's Order relies heavily on the fact that Capital One had a pre-existing SOW with Mandiant, *see* Order at 7-8, 11-14, it was also true in *Experian* that Mandiant had previously done work for Experian. *See* 2017 WL 4325583, at *3. That fact did not destroy work product protection in *Experian* because "Mandiant's previous work for Experian was separate from the work it did for Experian regarding this particular data breach." *Id.* So too here—in the two years preceding the Cyber Incident, Mandiant did not do any incident response work for Capital One and instead provided only training and consulting services. *See* Blevins Decl. ¶¶ 6-7, 9; Palombo Decl. ¶ 15; Caputo Decl. ¶ 4. The work Mandiant did before the Cyber Incident was thus "separate from the work it did ... regarding this particular data breach." 2017 WL 4325583, at *3; *see* Palombo Decl. ¶¶ 11, 13-15.[9]

[9] The circumstances surrounding Mandiant's work for Debevoise distinguish this case from the two cases on which the Order relies, *In re Premera Blue Cross Customer Data Sec. Breach Litigation*, 296 F. Supp. 3d 1230 (D. Or. 2017), and *In re Dominion Dental Servs. USA, Inc. Data Breach Litigation*, 429 F. Supp. 3d 190 (E.D. Va. 2019). *See* Order at 10-13. In *Premera*, the evidence showed that Mandiant "was performing an ongoing investigation under Premera's supervision *before outside counsel became involved*" and there was no "showing that Mandiant changed the nature of its investigation" after counsel became involved. 296 F. Supp. 3d at 1245–46 (emphasis added). Similarly, *Dominion Dental* found that defendants had not shown that anticipated litigation affected the purpose of Mandiant's work. *See* 429 F. Supp. 3d at 195. Indeed, the post-breach agreement Mandiant entered with Dominion Dental's outside counsel did not suggest any change in Mandiant's work because, unlike here, outside counsel *was also* a party to

Additionally, as in *Experian* and *Target*, Capital One conducted internal business investigations parallel to Debevoise's and Mandiant's protected investigations, which further demonstrates the distinction between Mandiant's protected, legal work and Capital One's ordinary-course, business investigation. *See Target*, 2015 WL 6777384, at *2 ("[F]ollowing the data breach, there was a two-track investigation," one of which was an "ordinary-course investigation" and the other of which was intended to "provide Target with legal advice"); *Experian*, 2017 WL 4325583, at *2 (noting the existence of separate "internal investigation" and "remediation efforts"); Mot. Ex. 13 at 21-22 (listing multiple internal investigations conducted by Capital One).[10] [redacted] and Capital One does not claim that they are privileged or protected in their entirety.

In fact, on June 4, 2020, Capital One produced documents relating to two of these investigations—Project Star and Project Refraction—including the final Project Star Post-Incident Report. *See* Ex. 2. Unlike these internal investigations performed for business and regulatory purposes, Mandiant's investigation and Report were performed for outside counsel and driven by the prospect of litigation arising from the Cyber Incident.

2. The Magistrate Judge incorrectly treated the pre-existing SOW between Capital One and Mandiant as dispositive.

The Magistrate Judge concluded that the pre-existing SOW between Capital One and Mandiant was nearly dispositive. He reasoned that the Mandiant Report was not work product because Mandiant could have conceivably provided the same "incident response services . . . in

---

the pre-breach contract for incident response services. *Id.* at 191-92. Finally, months passed between the time when Mandiant concluded its investigation into the Dominion Dental breach (May 2019) and the filing of the lawsuit in that case (August 2019). *See id.* at 191.

[10] *Experian*, *Target*, and this case can also be contrasted with *Dominion Dental* in that the court there emphasized the lack of "a two-track investigation," meaning Mandiant's report was "the only report" on the *Dominion Dental* data breach. *See Dominion Dental*, 429 F. Supp. 3d at 195.

substantially similar form even if there was no prospect of litigation." Order at 7. But even if Mandiant *could have performed* incident response services for Capital One under the prior SOW absent litigation, the undisputed evidence is that Mandiant did not perform any incident response work related to the Cyber Incident until *after* it was retained under a superseding engagement with Debevoise. *See* Palombo Decl. ¶ 15; Cantwell Decl. ¶ 6; Caputo Decl. ¶¶ 4, 11. It also does not follow that simply because Mandiant could have performed incident response services pursuant to the prior SOW, the services Mandiant actually *did perform* for Debevoise pursuant to the superseding engagement were not for the purposes of litigation.

In concluding otherwise, the Magistrate Judge elevated the test for work product applied in *RLI Insurance Co. v. Conseco, Inc.*, 477 F. Supp. 2d at 748, over the Fourth Circuit's "because of" test. *See* Order at 7 ("Therefore, the determinative issue is whether the Mandiant Report would have been prepared in substantially similar form but for the prospect of [the] litigation."). But while useful in some cases, the *RLI* standard does not displace the Fourth Circuit's controlling "driving force" test. *See Nat'l Union*, 967 F.2d at 984.[11] And here, litigation clearly was the driving force behind the preparation of the Mandiant Report. *See supra* pp. 13–16.

Even if the *RLI* test were relevant, the Magistrate Judge misapplied it. The Magistrate Judge's reliance on the preexisting SOW between Capital One and Mandiant was misplaced. That

[11] The *RLI* standard appears to be most useful in cases where the purported work product resembles documents the party creates in the ordinary course of its business, such as insurance claims files. *See, e.g.*, *RLI Ins. Co.*, 477 F. Supp. 2d at 749 (documents related to D&O insurer's review of claim for coverage arising from settlement of shareholder lawsuits); *see also Botkin v. Donegal Mut. Ins. Co.*, No. 5:10-cv-00077, 2011 WL 2447939, at *3–4 (W.D. Va. June 15, 2011) (appraisal obtained by insurer to form basis of settlement offer was protected work product, even though "settling claims is part of [insurer's] ordinary course of business," because insurer would not have obtained appraisal but for "desire to negotiate a settlement and avoid the risk and cost of litigation"). But here, Mandiant did not perform cybersecurity investigations for Capital One on an ongoing basis for business purposes.

document only broadly outlines the general types of incident response services that *might* be needed *in the event of* a data security incident—it does not specify the particular services to be provided in any detail. *See* Palombo Decl. ¶ 10 (noting that "the SOWs which Mandiant and Capital One entered into only describe the services at a high level" and that the "specifics" of any particular engagement would be "determined on a case-by-case basis"). The SOW thus does not bear on the key question here: whether litigation was the driving force behind the specific incident response services Mandiant performed for Debevoise in the wake of the Cyber Incident.

Confirming that litigation was that driving force, Mandiant's investigation and report would have been very different if Capital One had engaged Mandiant to investigate the Cyber Incident for *business* purposes. Caputo Decl. ¶¶ 3, 12. In that scenario, for example, Mandiant's investigation would have focused on remediation, as opposed to causation issues pertinent to legal liability determinations. *Id.* ¶ 12; *see also* Palombo Decl. ¶¶ 4-7 (explaining that when Mandiant is engaged by counsel, its focus is typically "assist[ing] in developing facts that will be used to defend the client in anticipated litigation related to a cybersecurity incident," whereas in engagements directly with the affected company, Mandiant and the Company set the investigative priorities). Additionally, absent the risk of litigation, Mandiant would not have worked with Capital One's legal department or outside counsel, but with Capital One's Cyber organization, and Mandiant's findings would have been reported to a wider segment of Capital One's business employees. Caputo Decl. ¶ 12. Finally, since Capital One hired Debevoise to obtain legal advice about anticipated litigation, the Mandiant Report would not "reflect the areas of inquiry that [Debevoise] direct[ed] Mandiant to focus on" and would not be "based on previously provided input from Debevoise regarding both the [R]eport's contents and the form it should take" absent that anticipated litigation. *See* Palombo Decl. ¶¶ 6, 16.

In short, the Magistrate Judge incorrectly relied on the *RLI* standard. Regardless, the Mandiant Report is protected work product even under that standard.

3. The Magistrate Judge's ruling has unworkable practical implications for heavily regulated companies that suffer data breaches.

The Magistrate Judge's reliance on the fact that Debevoise used a security vendor that was already familiar with Capital One's network infrastructure and that had a pre-existing relationship with Capital One overlooks the practical realities that highly regulated financial institutions face when a data breach occurs. When a vulnerability has been detected and potentially exploited, a company is under the gun to determine whether there has in fact been an intrusion, the scope of the intrusion, and whether any sensitive data was exfiltrated. Time is of the essence. Yet if Debevoise had attempted to use a vendor with whom Capital One did not have an existing relationship, it would have taken weeks to months to approve a new vendor due to bank data security and regulatory obligations, as opposed to the hours or days a company has to effectively respond to a potential data breach.

Capital One must comply with a "stringent regulatory framework" before granting a third-party vendor access to bank systems or data. Caputo Decl. ¶ 7. Capital One's vetting process, or Third-Party Risk Management ("TPRM") Program, entails performing a comprehensive risk assessment, negotiating the terms of the contract, and vetting the vendor by key internal stakeholders. *Id.* ¶ 8. Without a pre-existing contractual relationship, onboarding a new vendor under the TPRM Program "would take, conservatively, one to three months to complete." *Id.* ¶ 9. Even if done on an "emergency basis," the TPRM process takes "months"—which would have been far too long "[g]iven the emergency timeframe Debevoise was facing to understand the technical forensic findings" about the Cyber Incident. *Id.* ¶ 10.

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—particularly here, where Capital One had an urgent need to engage an expert to investigate the Cyber Incident, but would have been legally incapable of bringing a new forensic investigator into the fold for months.[12] 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. In crafting the work product doctrine, however, the Supreme Court sought to minimize exactly this sort of "[i]nefficiency, unfairness and sharp practices" that do not serve "the interests of the clients and the cause of justice[.]" *Hickman v. Taylor*, 329 U.S. 495, 511 (1947)

As commentators have recognized, requiring a company to hire an unfamiliar vendor to deal with a data breach "makes little practical sense."[13] Such a requirement would cause companies to waste precious time locating a vendor with available capacity, getting the proper business approvals, and then getting the vendor up to speed on the company's security infrastructure. While taking these steps might make any resulting report more likely to receive work product protection, the irony, of course, is that the associated delay would also

[12] Capital One's TPRM policies would apply to any vendor that requires access to its systems and data, regardless of whether that vendor is hired by Capital One directly or by outside counsel. *See* Caputo Decl. ¶¶ 6-10 (explaining any new vendor that Debevoise selected would have been required to undergo the TPRM approval process).

[13] Ben Kochman, *It's Getting Harder to Hide Consultants' Data Breach Reports*, Law360 (June 3, 2020) (attached as Exhibit 5).

unquestionably be used by plaintiffs as additional fodder for their challenges to the company's breach response and remediation efforts.

B. The Magistrate Judge Erred by Relying on Later Uses of the Mandiant Report to Determine the Purpose for which It Was Created.

1. That a document created in anticipation of litigation is later used for business purposes does not strip it of protection.

The second basis for the Magistrate Judge's ruling—that the Mandiant Report was used for business purposes—was error. The Magistrate Judge stressed that after it was created, the Mandiant Report was "provided to four different regulators," to Capital One's outside auditor, and to "several members of Capital One's cyber technical, enterprise services, information security and cyber teams." Order at 8, 10. It is well established, however, that a determination of work product protection is made as of the time the document is created, *see Chambers v. Allstate Ins. Co.*, 206 F.R.D. 579, 588 (S.D.W. Va. 2002) (focusing on "when Defendants reasonably anticipated litigation"), and that "material generated in anticipation of litigation may also be used for ordinary business purposes without losing its protected status" *Deloitte LLP*, 610 F.3d at 138. As the Ninth Circuit has explained, the "'because of' standard *does not consider whether litigation was a primary or secondary motive behind the creation of a document*. Rather, it considers the totality of the circumstances and affords protection when 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 that litigation.'" *In re Grand Jury Subpoena (Mark Torf/Torf Envtl. Mgmt.)*, 357 F.3d 900, 908 (9th Cir. 2004) (emphasis added) (citation omitted).

At the time Debevoise engaged Mandiant, the investigation's purpose was to assist Debevoise in providing legal advice in the face of impending litigation, not to support any business function. Cantwell Decl. ¶ 19. When complete, the Mandiant Report was initially shared only with Debevoise, which provided it to Capital One's legal team. *Id.* ¶ 20. That the Mandiant Report

was *later* shared with "select non-attorney employees who had a critical need to examine it," Capital One's regulators, and Capital One's auditor does not strip it of work product protection. Cantwell Decl. ¶ 21; *see Grand Jury Subpoena*, 357 F.3d at 910 (holding that "dual purpose" documents were entitled to work product protection because "their litigation purpose so permeate[d] any non-litigation purpose that the two purposes [could not] be discretely separated from the factual nexus as a whole"); *Adlman*, 134 F.3d at 1195 ("[A] document created because of anticipated litigation . . . does not lose work-product protection merely because it is intended to assist in the making of a business decision."); *In re Zetia (Ezetimibe) Antitrust Litig.*, No. 2:18-md-2836, 2019 WL 6122012, at *4 (E.D. Va. July 16, 2019) (recognizing materials prepared because of litigation retain work product status even if they are later used for "a business decision as well as a legal decision") (internal citation omitted).

The Ninth Circuit's decision in *Grand Jury Subpoena* is instructive. There, the government sought documents that were created both in anticipation of potential litigation with the EPA *and* for the non-litigation purposes of cleaning up contaminated sites and determining compliance with an environmental consent order. 357 F.3d at 908. As in this case, the documents at issue were prepared by an expert retained by counsel to assist in investigating the matter and to consult on cleanup efforts at the contaminated sites. *Id.* at 904. The government argued that the documents were not protected because they would have been created in any event to comply with a consent order. But the court rejected that argument:

> We conclude that the withheld documents, notwithstanding their dual purpose character, fall within the ambit of the work product doctrine. The documents are entitled to work product protection because, taking into account the facts surrounding their creation, their litigation purpose so permeates any non-litigation purpose that the two purposes cannot be discretely separated from the factual nexus as a whole.

Id. at 909-10. The *Experian* court engaged in a similar analysis. *See* 2017 WL 4325583, at *2 ("Mandiant conducted the investigation and prepared its report for Jones Day in anticipation of litigation, *even if that wasn't Mandiant's only purpose*." (emphasis added)). And the same is true here. Regardless of whether Capital One had other, business reasons to investigate the Cyber Incident, those reasons arose from the same set of facts that created the threat of litigation and occasioned Mandiant's investigation. The Mandiant Report was prepared in anticipation of litigation, was informed by Debevoise's needs and directives, and is therefore protected.

2. The limited, purportedly non-legal uses of the Mandiant Report do not undermine its entitlement to work product protection.

The Mandiant Report was initially shared only with Debevoise and Capital One's legal team. Cantwell Decl. ¶ 20; Blevins Decl. ¶ 18. That Capital One later disclosed the Mandiant Report to a limited number of recipients does not undermine its protected status, and the contrary conclusion in the Order constitutes legal error.

First, Capital One disclosed the Mandiant Report to its regulators—the OCC, FRB, FDIC, and CFPB—because it is obligated to do so. *See* Opp. at 10, 23 (explaining that Capital One "has a legal obligation to respond to requests from these regulators"); *see also* 12 U.S.C. §§ 248, 481, 1820, 5515 (setting forth the statutory examination powers of the FRB, OCC, FDIC, and CFPB, respectively). The Magistrate Judge's reliance on Capital One's disclosure of the Report to its regulators was contrary to law, as it violated Congress's directive that "[t]he submission [of work product] to the [CFPB or] any Federal banking agency . . . ***shall not*** be construed as waiving, destroying, ***or otherwise affecting*** any privilege such person may claim with respect to [the work product]." 12 U.S.C. § 1828(x)(1) (emphasis added); *see also Ak. Elec. Pension Fund v. Bank of Am. Corp.*, No. 14-CV-7126 (JMF), 2016 WL 6779901, at *4 (S.D.N.Y. Nov. 16, 2016) (holding

that disclosure of work product to banking regulator would not waive protection in light of the explicit directive in 12 U.S.C. § 1828(x)(1)).[14]

Second, Capital One disclosed the Mandiant Report to EY—and Debevoise instructed Mandiant to communicate with EY—in order to confirm that the Cyber Incident did not impact the integrity of Capital One's internal controls over financial reporting. Cantwell Decl. ¶¶ 13-14, 21. That disclosure did not change the litigation-focused purpose of the Mandiant Report or convert it into an ordinary-course document. *See Lawrence E. Jaffe Pension Plan v. Household Int'l, Inc.*, 237 F.R.D. 176, 181 (N.D. Ill. 2006) (holding attorney opinion letters provided to auditor were protected work product and rejecting argument that documents would have been prepared in any event due to public company reporting obligations).

Third, although Capital One shared the Mandiant Report with a small number of employees, distribution of the Mandiant Report was "tightly controlled," "monitored," and "logg[ed]" by Capital One's Senior Associate General Counsel Heather Caputo. *See* Caputo Decl. ¶ 13. Out of over 370 people in Capital One's Legal Department, only 21 employees received the Mandiant Report, each of whom was "actively engaged in [Capital One's] post-breach remediation, litigation, and regulatory response efforts." *Id.* ¶ 14. Further, only a handful of employees in Capital One's nearly 700-person Cyber Organization received the Mandiant Report. *See id.* ¶ 12. In all, only 31 non-legal employees received the Report in a company that employs over 50,000 people. *See id.* ¶¶ 14-15. Importantly, almost all of these employees were either (a) in

[14] By prohibiting regulatory submissions from "waiving, destroying, or otherwise affecting" a privilege determination, Congress excluded such submissions not only from a waiver analysis, but also from the determination of whether a document is protected in the first instance. To hold otherwise would fail to give independent meaning to "waiving," "destroying," and "otherwise affecting," contravening "the presumption 'that statutory language is not superfluous.'" *McDonnell v. United States*, 136 S. Ct. 2355, 2369 (2016).

Capital One's "control group" of "executives working together to address the fallout" from the Cyber Incident, or (b) had "key roles in enterprise-wide control or governance functions," such as "Risk, Audit, Accounting [or] Corporate Governance." *Id.* ¶¶ 16-17. Ultimately, if the Mandiant Report had been prepared for business purposes, it would have been widely shared with business employees. But it was not. *See Experian*, 2017 WL 4325583, at *2 (noting that "Mandiant's full report wasn't given to Experian's Incident Response Team"). The Magistrate Judge's reliance on the limited internal disclosures of the Mandiant Report thus was error. *See* Order at 9-10.

Finally, none of the other grounds the Magistrate Judge relied on provides a basis for destroying the Report's work product protection. The Order notes that the Mandiant Report was used "internally for Sarbanes Oxley" disclosures. *Id.* at 8. But while making Sarbanes Oxley disclosures is necessary for Capital One's business, ensuring compliance with federal law serves a distinctly legal purpose—including to minimize the risk of regulatory action and litigation. *Cf. Lawson v. FMR LLC*, 571 U.S. 429, 451 (2014) (noting that the purpose of the Sarbanes-Oxley Act is to "protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws" (internal citation omitted)).

The Order also reasoned that (i) the "retainer paid to Mandiant was considered a business-critical expense and not a legal expense at the time it was paid" and (ii) the Report was "referenced in a draft FAQs prepared by a senior vice president for finance." Order at 8. With respect to the classification of the expenses, the exhibit on which the Order relies *pre-dates* the Cyber Incident and refers only to the Mandiant retainer; it therefore is not probative of the nature of Mandiant's *post*-Cyber Incident investigation. *See* Mot. Ex. 3, at -185319. Additionally, that document makes clear that the "business-critical" designation merely denotes that a particular cost is top priority—or "P1." *See id*. Further, the expenses associated with Mandiant's work for Debevoise were

"designated as discovery and investigation costs related to the Cyber Incident" during Capital One's "routine year-end accounting reconciliation" process, and were "deducted against the budget for Capital One's legal department consistent with the nature of the work Mandiant performed." Watts Decl. ¶ 5. If the Mandiant Report were "commissioned for business purposes, Capital One's accountants could not have classified the expenses associated with it as legal expenses." Caputo Decl. ¶ 5. With respect to the "draft FAQs" that were attached as Exhibit 12 to Plaintiffs' Motion, *see* Mot. Ex. 12 (Dkt. 416-12, filed under seal); Order at 8 n.3, Capital One now clarifies that they were not used by Capital One personnel. *See* Caputo Decl. ¶ 20.[15]

II. THE COURT CANNOT SUSTAIN THE ORDER ON ALTERNATIVE GROUNDS.

If the Court concludes that the Mandiant Report is protected work product, it should set aside the Order because neither of Plaintiffs' alternative arguments—that Capital One waived protection over the Mandiant Report or that Plaintiffs' are entitled to the Report under Rule 26(b)(3)—has merit. While expressly stating it was unnecessary to reach the waiver issue in light of his conclusion that the Mandiant Report was not work product, the Magistrate Judge nonetheless stated that "the waiver argument may have some merit" based on a perceived lack of evidence "concerning the distribution of the Mandiant Report and what protections were taken to avoid

[15] The Order notes that the court in *Dominion Dental* found relevant that the defendant there included a reference to retaining Mandiant in a list of talking points. *See* Order at 12 (citing *In re Dominion Dental*, 429 F. Supp. 3d at 194). But the evidence in *Dominion Dental* showed that the talking points referencing Mandiant were included in an "incident response communications and support kit" that the defendant provided to its client for the purpose of reassuring customers. *See* 429 F. Supp. 3d at 194. The same is not true here—Capital One's draft FAQs were never used, and Capital One's public statements about the breach, such as its July 29, 2019 press release, specifically omitted any mention of Mandiant. *See* Dkt. 387-3 at 6-8.

having the Mandiant Report or the information therein disclosed to a person or entity in an adversarial relationship." Order at 7 n.2.[16] That suggestion is incorrect.

A. Capital One's Disclosures of the Mandiant Report Did Not Effect a Waiver.

As the Magistrate Judge noted, Capital One disclosed the Mandiant Report to three categories of users: (1) Capital One's four banking regulators; (2) Capital One's auditor, EY; and (3) a limited group of Capital One employees. Order at 4. None of these disclosures was a waiver.

Disclosure to Capital One's Banking Regulators. As noted, as a matter of federal law, Capital One's disclosure of the Mandiant Report to the FRB, OCC, CFPB, and FDIC cannot be construed as a waiver of the work product protection. *See* 12 U.S.C. § 1828(x) (stating that disclosure of "any information to the [CFPB], [or] any Federal banking agency . . . for any purpose in the course of any supervisory or regulatory process . . . ***shall not*** be construed as waiving, destroying, or otherwise affecting any privileges such person may claim with respect to such information" (emphases added)); 12 U.S.C. § 1813(z) (defining "Federal banking agency" as the OCC, FRB, and FDIC); *see also Ak. Elec. Pension Fund*, 2016 WL 6779901, at *4 (stating submissions of work product to "prudential" regulators would not waive privilege).[17]

[16] With respect to Plaintiffs' substantial need/undue hardship argument, the Magistrate Judge correctly suggested, but did not rule, that Plaintiffs had not made the required showing. *See* Order at 7 n.2. Indeed, Plaintiffs provided *zero* evidence to substantiate their argument that analyzing the source materials and historical data that Mandiant relied upon—which is indisputably available to them—or hiring an expert to do so would be an "undue hardship." *See, e.g.*, May 15, 2020 Hr'g Tr. 8:14-10:25 (failing to substantiate the "undue hardship" argument in oral argument). Moreover, Capital One has produced to Plaintiffs reports of certain of its internal investigations into the Incident, further undermining any undue hardship argument.

[17] Even if, as Plaintiffs claimed, the banking regulators had been investigating or considering an enforcement action against Capital One at the time they received the Report, the disclosure still could not effect a waiver because investigations and enforcement actions are part of the agencies' "regulatory process[es]." 12 U.S.C. § 1828(x).

Disclosure to EY. Capital One's disclosure of the Mandiant Report to its auditor, EY, did not waive work product protection. "The Fourth Circuit has clearly held that for a waiver to occur, the disclosure must be made freely and with the knowledge that [the] document is being passed to a party with adverse interests." *See Sheets v. Ins. Co. of N. Am.*, No. 4:04-cv-00058, 2005 WL 3006670, at *2 (W.D. Va. Nov. 8, 2005); *see also FEC v. Christian Coalition*, 178 F.R.D. 61, 77 (E.D. Va. 1998) (asking whether the recipient of work product was the party's "litigation adversary"). And as the District of Columbia Circuit has explained, the relationship between an independent auditor and its client *cannot* approach that of litigation adversaries: "[e]ven the threat of litigation between an independent auditor and its client can compromise the auditors' independence and necessitate withdrawal." *Deloitte LLP*, 610 F.3d at 140. Nor is there any risk that EY would provide the Mandiant Report to Capital One's litigation adversaries because "as an independent auditor, [it] has an obligation to refrain from disclosing confidential client information." *Id.* at 142 (citing AICPA Code of Prof'l Conduct Rule 301.01).[18] The sole case Plaintiffs relied on that might arguably find waiver in this context, *Medinol, Ltd. v. Boston Sci. Corp.*, 214 F.R.D. 113 (S.D.N.Y. 2002), "has been almost uniformly rejected as adopting far too restrictive of a view regarding the circumstances under which a waiver can occur." *In re Weatherford Int'l Secs. Litig.*, No. 11 CIV 1646 (LAK/JCF), 2013 WL 12185082, at *5 (S.D.N.Y. Nov. 19, 2013) (citation omitted).

Internal Disclosures. The Magistrate Judge cited Capital One's disclosures of the Report to approximately 50 Capital One employees, 31 of whom were not part of Capital One's legal

[18] *See also Int'l Design Concepts, Inc. v. Saks, Inc.*, No. 05-cv-4754 (PKC), 2006 WL 1564684, at *3 (S.D.N.Y. June 6, 2006) (no waiver where outside counsel's investigative findings were shared with independent auditor); *Frank Betz Assocs., Inc. v. Jim Walter Homes, Inc.*, 226 F.R.D. 533, 535 (D.S.C. 2005) (work product shared with outside auditor still protected); *Merrill Lynch & Co. v. Allegheny Energy, Inc.*, 229 F.R.D. 441 (S.D.N.Y. 2004) (similar).

department. *See* Order at 4-5; May 15, 2020 Hr'g Tr. 22:9-12; *see also* Caputo Decl. ¶ 15. He also found a "lack of evidence . . . concerning the distribution of the Mandiant Report" and the "protections . . . taken to avoid having the Mandiant Report" disclosed to an adversary. But, as set forth in Capital One's Opposition and demonstrated by the list of recipients attached thereto as Exhibit 2, all of the recipients of the Mandiant Report were tracked and logged. Opp. at 9; Opp. Ex. 2 (Dkt. 435-5) at 8-9; *see also* Caputo Decl. ¶ 13 (explaining how she "vetted specific employee requests for" the Report). Not every recipient was granted permission to print the Report, and such permission was only granted, if at all, with the "express understanding" that the Report was to be "safely guarded, kept confidential, and not disseminated." Caputo Decl. ¶ 13. Regardless, the pertinent inquiry is whether the Report was disclosed to Capital One's "litigation adversary," *FEC*, 178 F.R.D. at 77, and none of Capital One's employees are or will become Capital One's adversaries in litigation arising out of the Cyber Incident. *See, e.g.*, *Rockwell Automation, Inc. v. Radwell Int'l, Inc.*, No. 15-5246(RBK/JS), 2019 WL 1864198, at *3 (D.N.J. Apr. 25, 2019) ("Plaintiff's employees . . . were not plaintiff's adversaries and therefore no waiver occurred."); *In re Weatherford*, 2013 WL 12185082, at *5 (no waiver based on disclosure to audit committee because it "is part of the company"). It would be anomalous to conclude that disclosures to a party's own employees waive work product protection when disclosures to a third party only do so in such limited circumstances. Accordingly, Capital One's disclosure of the Report to select employees did not waive work product protection.

B. Capital One's Statements About the Cyber Incident and Its Remediation Did Not Effect an "At Issue" Waiver.

Plaintiffs also advocated for waiver on a second ground—that Capital One put the Mandiant Report "at issue" in its public statements about the Cyber Incident and in its discovery responses. *See* Mot. at 19 (arguing Capital One's statement that it "immediately fixed the issue"

and its descriptions of its remedial efforts put the Mandiant Report at issue based on speculation that such information is "addressed in the Mandiant Report"); *id.* (arguing interrogatory response indicating Paige Thompson was the only hacker to exploit the vulnerability in question put the Mandiant Report at issue). An "at issue" waiver can occur only where the party asserting protection places the protected information "directly at issue." *See Smith v. Scottsdale Ins. Co.*, 40 F. Supp. 3d 704, 725 (N.D.W. Va. 2014); *Black & Decker Corp. v. United States*, 219 F.R.D. 87, 92 (D. Md. 2003). As the Magistrate Judge correctly noted, neither of the statements upon which Plaintiffs rely reference or in any way indicate that the Mandiant Report was the basis for the information. *See* May 15, 2020 Hr'g Tr. 7:19-22 ("It doesn't say Mandiant – we, we have hired an independent third party, Mandiant, a well-recognized entity in this field, to take this, and they have certified that it's been fixed."). Accordingly, no "at issue" waiver occurred.

CONCLUSION

For the reasons explained herein, Capital One respectfully asks this Court to set aside the Order compelling Capital One to produce the Mandiant Report.

Dated: June 9, 2020

Respectfully Submitted,

/s/

David L. Balser (*pro hac vice*)
S. Stewart Haskins II (*pro hac vice*)
John C. Toro (*pro hac vice*)
Kevin J. O'Brien (VSB No. 78886)
Robert D. Griest (*pro hac vice*)
KING & SPALDING LLP
1180 Peachtree Street, N.E.
Atlanta, Georgia 30309
Telephone: (404) 572-4600
Facsimile: (404) 572-5140
dbalser@kslaw.com
shaskins@kslaw.com
jtoro@kslaw.com
kobrien@kslaw.com
rgriest@kslaw.com

Defendants' Lead Counsel

Robert A. Angle (VSB No. 37691)
Tim St. George (VSB No. 77349)
Jon S. Hubbard (VSB No. 71089)
Harrison Scott Kelly (VSB No. 80546)
TROUTMAN SANDERS LLP
1001 Haxall Point
Richmond, VA 23219
Telephone: (804) 697-1200
Facsimile: (804) 697-1339
robert.angle@troutman.com
timothy.st.george@troutman.com
jon.hubbard@troutman.com
scott.kelly@troutman.com

Mary C. Zinsner (VSB No. 31397)
TROUTMAN SANDERS LLP
401 9th Street, NW, Suite 1000
Washington, DC 20004
Telephone: (703) 734-4334
Facsimile: (703) 734-4340
mary.zinsner@troutman.com

Defendants' Local Counsel

CERTIFICATE OF SERVICE

I hereby certify that on June 9, 2020, I caused the foregoing document to be filed with the Clerk of Court using the CM/ECF system, which will send notice of electronic filing to all counsel of record.

/s/
David L. Balser

Counsel for Capital One