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 OPPOSITION TO PLAINTIFF'S MOTION TO COMPEL PRODUCTION OF MANDIANT REPORT AND RELATED MATERIALS

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
Tel.: (404) 572-4600
Fax: (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

INTRODUCTION

Within days of discovering the data breach at the center of this litigation (the "Cyber Incident"), Capital One hired the law firm of Debevoise & Plimpton ("Debevoise") to investigate the circumstances surrounding the Cyber Incident, to provide legal advice to Capital One and its Board of Directors concerning the Cyber Incident, and to help the company prepare for and defend against the onslaught of litigation and regulatory inquiries that Capital One anticipated would (and did) follow immediately after the company announced the Cyber Incident.

To aid in its privileged investigation, Debevoise engaged FireEye, Inc., d/b/a Mandiant ("Mandiant"), one of the nation's preeminent cybersecurity consulting firms. Among other things, Mandiant helped Debevoise understand and interpret technical issues it encountered during its investigation and performed a "red team" exercise to assess the remediation of the vulnerability that led to the Cyber Incident. These services were important to Debevoise's legal counsel to the company. At all times, Debevoise directed and supervised Mandiant's work.

As part of its investigation, Debevoise directed Mandiant to prepare a report summarizing its findings about the Cyber Incident and the technical factors that allowed the hacker to penetrate Capital One's security (the "Mandiant Report"). Mandiant prepared its Report as part of Debevoise's investigation into the Incident, and the Mandiant Report was incorporated into Debevoise's own final report to Capital One's Board of Directors. By the time Mandiant issued its report in September 2019, Capital One had been sued in over sixty putative class actions arising from the Cyber Incident. In these circumstances, the Mandiant Report is protected attorney work product—a conclusion numerous courts have reached in cases where Mandiant served a nearly identical role. *See, e.g.*, *In re Experian Data Breach Litig.*, No. SACV 15-01592 AG (DFMx), 2017 WL 4325583, at *2 (C.D. Cal. May 18, 2017); *In re Arby's Rest. Grp., Inc. Data Sec. Litig.*, No. 1:17-mi-55555-WMR (N.D. Ga. March 25, 2019), Doc. No. 453.

Plaintiffs contend that the Court should compel production of the Mandiant Report because (1) Capital One and Mandiant had a preexisting contract for incident response services dating back to 2015, which Plaintiffs argue vitiates the work product protection attaching to Debevoise's post-breach retention of Mandiant; (2) Capital One waived the protection by disclosing the Mandiant Report to its supervisory banking regulators—the Office of the Comptroller of the Currency ("OCC"), the Federal Reserve Board ("FRB"), the Federal Deposit Insurance Company ("FDIC"), and the Consumer Financial Protection Bureau ("CFPB")—and to its outside auditor, Ernst & Young ("E&Y'); and, (3) Plaintiffs claim to have a "substantial need" for the Mandiant Report and assert they cannot otherwise obtain its substantial equivalent without "undue hardship." These arguments lack merit.

First, in the roughly two years that preceded the Cyber Incident, Mandiant did ***no*** data breach response work for Capital One. During that time period, Mandiant provided only consulting and training services to Capital One. But the work Mandiant did after the Cyber Incident had an entirely different scope and purpose. Debevoise retained Mandiant just six days before the first class action lawsuit arising out of the Cyber Incident was filed against Capital One. Mandiant's post-breach forensic investigation was part of Debevoise's broader investigation of the Cyber Incident, and when Mandiant completed its Report, Capital One was already defending dozens of class action lawsuits arising out of the Cyber Incident.

Plaintiffs' assertion that Capital One retained Debevoise to shroud Mandiant's work in privilege is both unfounded and wrong. Debevoise performed an extensive investigation into the Cyber Incident, conducting substantial document review and interviewing over 160 witnesses over the course of approximately five months—all of which culminated in a final report Debevoise delivered to Capital One's legal department and Board of Directors. And Debevoise engaged

Mandiant—well-recognized cybersecurity experts who frequently consult in major data breach cases—to prepare a Report that was an important component of Debevoise's legal work for the company. In short, Debevoise was not hired as part of some ploy to protect discoverable information about business matters under the cloak of privilege. Mandiant's Report was prepared for Capital One's legal counsel in anticipation of litigation and is therefore protected attorney work product.

Second, Plaintiffs' argument that Capital One waived protection over the Mandiant Report by sharing it with banking regulators and its auditor fails. Capital One's disclosure of the Report to its banking regulators did not waive protection as a matter of law. *See* 12 U.S.C. § 1828(x) (disclosure of "any information to … any Federal banking agency … for any purpose in the course of any supervisory or regulatory process …. ***shall not*** be construed as waiving" an applicable privilege). Moreover, disclosure of work product to a third-party results in a waiver only if it "creates a substantial risk that [the work product] will be received by an adversary." *Cont'l Cas. Co. v. Under Armour, Inc.*, 537 F. Supp. 2d 761, 772 (D. Md. 2008). Applying that standard here, neither Capital One's disclosure of the Mandiant Report to its banking regulators—nor its disclosure to its auditors—waived work product protection, because neither disclosure significantly increased the odds that Capital One's litigation adversaries would obtain the report. *See, e.g.*, *U.S. v. Deloitte LLP*, 610 F.3d 129, 140 (D.C. Cir. 2010) (disclosure of work product to auditor did not waive protection because "as an independent auditor, Deloitte cannot be Dow's adversary"); *Ak. Elec. Pension Fund v. Bank of Am. Corp.*, 14-CV-7126 (JMF), 2016 WL 6779901, at *4 (S.D.N.Y. Nov. 16, 2016) (disclosure of work product to bank regulator would not waive protection).

Finally, the Court should reject Plaintiffs' invitation to compel production of the Mandiant Report under Rule 26(b)(3)(A). The Mandiant Report is core opinion work product prepared to help counsel develop its legal theories about the Cyber Incident and strategy for defending litigation. The Report should thus be protected as inviolate. But even if the Mandiant Report were purely factual work product, Plaintiffs fail to show a "substantial need" for the Report or "undue hardship" from not having it. As part of the discovery process, Capital One has already produced (and continues to produce) documents and information sufficient to enable Plaintiffs to determine the root cause of the Cyber Incident. Nothing prevents Plaintiffs from using those documents and information to conduct their own forensic investigation and analysis. The Court should not let Plaintiffs co-opt Capital One's work product just because it may be more "efficient" for them to do so. *See* Pls.' Motion to Compel Br. ("Mot.") at 21.

For these reasons, the Court should deny Plaintiffs' motion to compel.

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"). Mot. Ex. 1, Master Services Agreement (executed Nov. 24, 2015), CAPITALONE_MDL_000258941 at -258941. Beginning in 2015, Capital One and Mandiant executed periodic SOWs for "incident response services" that may be needed during a given year. Mot. Ex. 2, Statement of Work (executed Jan. 7, 2019), CAPITALONE_MDL_000097222 at -97223; Declaration of Jeffrey Blevins II ¶ 4. 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. 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.

In the two years before the Cyber Incident, Capital One did not need Mandiant to provide any incident response services. Blevins Decl. ¶ 7. So, instead of wasting the retainer paid to Mandiant for those years, Capital One and Mandiant agreed that the retainer amounts would be used for Mandiant to perform other services, such as training and consulting work. *Id.* ¶ 9. For example, when it became clear in 2018 that Mandiant's retainer fee would not be needed for incident response services, Capital One asked Mandiant to conduct a review of Capital One's cyber incident "preparedness." *See id.* ¶ 10. The review was designed to evaluate Capital One's policies and procedures for responding to potential cybersecurity incidents. *Id.* At the end of that review, Mandiant developed a roadmap detailing how Capital One could improve its incident response posture. *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 similar consulting services for Mandiant to provide, including a Windows Enterprise Incident Response training course. *Id.* But this work was put on hold after Capital One discovered the Cyber Incident in July 2019. *Id.*

B. Mandiant's Work for Debevoise Following the Cyber Incident.

On July 19, 2019, Capital One confirmed that the Cyber Incident had occurred. The company immediately initiated numerous internal investigations and reviews (some privileged, some not) into the Cyber Incident and its causes. *See* Mot. Ex. 13 at 21-22 (listing multiple internal investigations). 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. Instead, the company retained Debevoise on July 20, 2019 to conduct a privileged investigation into the circumstances that gave

rise to the Cyber Incident and 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. Declaration of Helen Cantwell ¶¶ 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.

Shortly after being retained by Capital One, Debevoise engaged Mandiant to assist in its privileged investigation. *Id.* ¶ 6. Mandiant did not perform any work regarding the 2019 Cyber Incident until it was engaged and directed by Debevoise. *Id.*; Blevins Decl. ¶ 14. And although Capital One had previously entered into an MSA with Mandiant, Debevoise's engagement of Mandiant was separate from any previous work Mandiant had done for the company. *Compare* Cantwell Decl. Ex. A, Debevoise-Mandiant-Capital One Engagement Letter, CAPITALONE_MDL_000393993 at -393993 (directing 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).

The agreement signed by Debevoise, Mandiant, and Capital One on July 24, 2019 confirmed Mandiant's new role, making clear that Debevoise had engaged Mandiant to provide forensic and incident response services to assist in Debevoise's privileged investigation and provision of legal advice to Capital One. Cantwell Decl. Ex. A at -393993, -393994. The agreement specifically notes that Mandiant was retained to "provide services and advice, *as*

directed by [Debevoise]" in numerous technical areas. *Id.* at -393993 (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, CAPITALONE_MDL_000392934 at -392934, -392935. Just four days later, the first putative class action lawsuit arising out of the Cyber Incident was filed against Capital One. *See* Dkt. 1, *Baird v. Capital One Financial Corporation*, No. 1:19cv979 (LMB/JFA) (E.D. Va. filed July 30, 2019). Debevoise—*not* Capital One—directed and oversaw all aspects of Mandiant's work related to the Cyber Incident. Cantwell Decl. ¶ 12; Blevins Decl. ¶ 12.

Mandiant played a critical role in Debevoise's privileged and work product protected investigation into the Cyber Incident, assisting the firm in assessing the technical aspects of the Cyber Incident. Cantwell Decl. ¶ 15; Cantwell Decl. Ex. A at -393993. Specifically, Mandiant assisted Debevoise by (1) helping Debevoise understand and interpret the technical matters it encountered in its review of documents and certain witness interviews; (2) consulting on specific sub-investigations Debevoise conducted on various technical matters; and (3) performing a "red team" exercise to assess the vulnerability that led to the Cyber Incident. Cantwell Decl. ¶ 16. Debevoise's ability to provide legal advice was significantly enhanced by Mandiant's technical advice. *Id.* ¶ 17.

Though the work Mandiant performed at Debevoise's direction was separate from the existing relationship between Mandiant and Capital One, that existing relationship allowed Debevoise to promptly engage Mandiant and bypass the administrative hurdles associated with vetting a new third-party service provider. *Id.* ¶¶ 9-10; Blevins Decl. ¶ 13. As a federally regulated financial institution that stores sensitive information, Capital One has a rigorous process for vetting

third-party service providers before they can gain access to Capital One's systems. Blevins Decl. ¶ 5. Because Capital One had already vetted Mandiant as a service provider, Mandiant was able to promptly gain access to Capital One's secure systems to perform the work Debevoise hired it to do. *See id.* ¶¶ 5, 13; Cantwell Decl. ¶ 10.

Like other vendors retained by Debevoise, Mandiant billed Capital One directly. Cantwell Decl. ¶ 11. Given that Mandiant had an existing relationship with Capital One and that the retainer paid to Mandiant for 2019 had not been exhausted, Mandiant was initially paid out of that retainer. Declaration of David Watts ¶ 3. But once those funds were exhausted, Mandiant's additional payments were made from the budget for Capital One's legal expenditures in connection with the Cyber Incident.[1] *Id.* ¶ 4. 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 done for outside counsel (*see* Cantwell Decl. ¶ 11).

As contemplated in the engagement agreement, Debevoise directed and supervised all of Mandiant's work on the Cyber Incident. *See* Ex. 1, Email from Cyber to Mandiant (Sept. 9, 2019), CAPITALONE_MDL_000392727 at -392727 ("At this point since Cyber isn't directing the work or resources, can you please send these types of messages to [Capital One's in-house counsel] . . . ."). Of course, Mandiant necessarily had to communicate with certain Capital One employees in the course of its investigation, but it did so under Debevoise's direct supervision. Blevins Decl. ¶ 17; Cantwell Decl. ¶ 18. Mandiant did not share its analysis with Capital One employees. Blevins Decl. ¶ 18; Cantwell Decl. ¶ 20.

[1] Though the additional funds Mandiant was paid 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 deducted from the company's legal budget after a routine year-end accounting of the expenses incurred in connection with the Cyber Incident was conducted. *See id.* ¶ 5.

Debevoise also included Mandiant in limited communications with E&Y—Capital One's independent auditor. Cantwell Decl. ¶ 13. These communications, which occurred roughly five weeks before Mandiant issued its final report to Debevoise on September 4, 2019, were limited to Mandiant's confirmation of discrete facts necessary for E&Y to conclude that the Cyber Incident had no impact on Capital One's financial systems or internal controls over financial reporting. *Id.* ¶ 14.

Mandiant issued its Report advising Debevoise on technical issues relating to the Cyber Incident in order to assist Debevoise in providing legal advice to Capital One and preparing for the litigation the company was already facing. *Id.* ¶ 19. Mandiant's Report was initially shared only with Capital One's legal team. *Id.* ¶ 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* Ex. 2, Email from J. Toro to J. Dent (May 5, 2020) (attaching a list of recipients of the Mandiant Report in response to Plaintiffs' supplemental discovery demands). In a company that employs more than 600 people in its Cyber organization[2] alone and thousands more in other information technology functions, only 32 non-lawyers were given access to the Report. *Id.*; *see also* Mot. Ex. 3, Cyber Monthly Financial Review (Feb. 22, 2019), CAPITALONE_MDL_000185308 at -185311, -185312 (stating the number of Cyber employees as of January 2019). Many of these individuals were employed in accounting, risk management, and audit functions (all areas related to legal and advisory services). Only a handful of recipients were members of the Cyber organization. That so few business employees at Capital

[2] 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.

One saw the Mandiant Report belies Plaintiffs' assertion that the Report was created primarily for "business purposes."

Disclosure of the Report outside the company was even more limited. Capital One provided the Report to four federal bank regulators—the OCC, the FRB, the FDIC, and the CFPB. Capital One has a legal obligation to respond to requests from these regulators, and, under the Financial Services and Regulatory Relief Act of 2006 ("FSRRA"), its disclosures to these regulators may "not be construed as waiving" work product protection over the Mandiant Report. 18 U.S.C. § 1828(x)(1). Moreover, Capital One's communications with these regulators are independently protected by the bank examiner privilege. *See* 12 C.F.R. § 4.36 *et seq*. (OCC); 12 C.F.R. § 261.20 *et seq*. (FRB); 12 C.F.R. § 309.1 *et seq*. (FDIC); 12 C.F.R. § 1070.40 *et seq*. (CFPB). E&Y also received a copy of the Report in connection with its role as Capital One's auditor. Cantwell Decl. ¶ 21.

LEGAL STANDARD

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); *United States v. Nobles*, 422 U.S. 225, 238-39 (1975). In the Fourth Circuit, a document that is "prepared *because of* the prospect of litigation" qualifies for work product protection and is not discoverable. *Nat'l Union Fire Ins. Co. of Pittsburgh v. Murray Sheet Metal Co.*, 967 F.2d 980, 984 (4th Cir. 1992). The Mandiant Report easily meets this standard.

ARGUMENT

I. THE MANDIANT REPORT IS PROTECTED WORK PRODUCT.

A. The Mandiant Report Bears All of the Hallmarks of Protected Work Product.

The essential facts surrounding Mandiant's engagement confirm that the Mandiant Report and related working papers constitute protected work product. To determine whether a document

was prepared "because of" the prospect of litigation, this Court must first ask whether Capital One "face[d] an actual claim or a potential claim following an actual event or series of events that reasonably could result in litigation." *Nat'l Union*, 967 F.2d at 984. There is no question that the Cyber Incident was the type of event that Capital One knew would lead to litigation. Prior cybersecurity incidents suffered by similarly prominent companies and involving similar numbers of consumers had, without exception, been followed by waves of consumer litigation.[3] The Cyber Incident prompted a similar response—61 putative class action lawsuits were filed by 263 plaintiffs. In fact, Capital One was sued within 24 hours of announcing the Cyber Incident, and nearly 60 putative class actions were already pending by the time Mandiant completed its Report.

The second prong of the Fourth Circuit's "because of" inquiry asks whether the document "would not have been prepared in substantially similar form but for the prospect of that litigation." *E.I. Du Pont de Nemours & Co. v. Kolon Indus., Inc.*, No. 3:09cv58, 2010 WL 1489966, at *3 (E.D. Va. Apr. 13, 2010) (quoting *RLI Ins. Co. v. Conseco, Inc.*, 477 F. Supp. 2d 741, 748 (E.D. Va. 2007)). While "materials prepared in the ordinary course of business" are not entitled to work product protection, *Nat'l Union*, 967 F.2d at 984, there is no bright-line test to distinguish materials prepared in anticipation of litigation from those prepared in the ordinary course, so courts in this Circuit take "a 'case-by-case' approach," *Lewis v. Richland Cty. Recreation Comm'n*, No. 3:16-cv-2884, 2018 WL 4596119, at *6 (D.S.C. Sept. 25, 2018) (quoting *Kidwiler v. Progressive*

[3] *See, e.g.*, *In re Marriott Int'l, Inc. Customer Data Sec. Breach Litig.*, No. 19-md-2879, 2020 WL 869241, at *2 (D. Md. Feb. 21, 2020) (Marriott data breach that involved nearly 383 million guest records); *In re Equifax Inc. Customer Data Sec. Breach Litig.*, No. 1:17-md-2800 (N.D. Ga. Mar. 17, 2020), ECF No. 1029 at 2 (Equifax data breach involving 147 million consumers); *In re Yahoo! Customer Data Sec. Breach Litig.*, No. 5:16-md-2752 (N.D. Cal. Jan. 31, 2020), ECF No. 414 at 6 (Yahoo! data breach that affected 194 million users); *In re Anthem, Inc. Customer Data Sec. Breach Litig.*, No. 5:15-md-2617 (N.D. Cal. Aug. 15, 2018), ECF No. 1046 at 4 (Anthem data breach involving over 79 million consumers).

Paloverde Ins. Co., 192 F.R.D. 536, 542 (N.D.W. Va. 2000)). Some of the relevant factors include (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. *Id.*

Here, *all* of the circumstances surrounding Mandiant's investigation support the conclusion that the Mandiant Report is protected work product. The engagement agreement between Debevoise, Mandiant, and Capital One expressly provides that Mandiant's work would be "as directed by Counsel," that the "Services under this Letter are done at Counsel's request," and that "all Deliverables … shall be properly communicated to … [and] delivered to Counsel," "[n]otwithstanding any prior agreements between Mandiant and [Capital One]." Cantwell Decl. Ex. A at -393993. The engagement letter also states that "the purpose of the Services under this Letter is to enable Counsel to render legal advice to client in anticipation of litigation or a regulatory inquiry." *Id.* The subject matter of the Mandiant Report was a forensic analysis of the Cyber Incident—which is also the subject of sprawling litigation and related regulatory proceedings—and the engagement agreement was entered into on July 24, 2019, just five days after Capital One confirmed the intrusion, and five days before the public announcement of the Cyber Incident, which triggered a deluge of litigation. *See* Cantwell Decl., Ex. A at -393993, -393994. Mandiant and Debevoise thereafter continued their work, and Mandiant completed its Report months later, at a time when this litigation was underway. Overall, the Mandiant Report was designed to give Capital One's outside counsel a reliable and expert understanding of the Cyber Incident so that counsel could effectively provide advice to Capital One in anticipation of litigation. *See* Cantwell Decl. ¶ 19

This is a role that Mandiant frequently plays in data breaches such as this, and numerous courts have held that reports like the Mandiant Report here are work product protected from disclosure. *See, e.g.*, *Arby's*, No. 1:17-mi-55555-WMR, Doc. No. 453 (denying motion to compel Mandiant report); *In re Experian*, 2017 WL 4325583, at *2 (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).

Experian involved facts strikingly similar to those here. Experian retained a law firm (Jones Day) for legal advice following a data breach. 2017 WL 4325583, at *2. "Jones Day then hired Mandiant to conduct an expert . . . analysis of the attack" that caused the breach, the purpose of which was "to help Jones Day provide legal advice to Experian regarding the attack." *Id.* Mandiant delivered the report to Jones Day, which in turn delivered it to Experian for the purpose of "develop[ing] their legal strategy." *Id.* The court found that "but for the anticipated litigation, the report wouldn't have been prepared in substantially the same form or with the same content," and concluded it was protected from disclosure by the work product doctrine. *Id.* at *2-*3. The same is true here.

Plaintiffs make much of the fact that Capital One had previously engaged Mandiant to perform other work relating to cybersecurity and incident response. *See, e.g.*, Mot. at 12, 14. They incorrectly claim that because Mandiant had an existing relationship with Capital One, the work Mandiant did at Debevoise's direction under a separate engagement cannot be protected from disclosure. *Id.* at 2.[4] Not only is this argument incorrect, but the facts Plaintiffs point to were also

[4] Taken to its logical conclusion, Plaintiffs' argument would lead to the absurd result that Debevoise would have been forced to engage a cybersecurity expert having no prior relationship with Capital One to protect the expert's work from disclosure in litigation. Adopting Plaintiffs'

present in *Experian*: there, Mandiant had previously done work for Experian, but the Court found that "Mandiant's previous work for Experian was separate from the work it did for Experian regarding this particular data breach." *Experian*, 2017 WL 4325583, at *3.

Likewise, Capital One did not use Mandiant for *any* incident response work in the two years prior to the Cyber Incident. Blevins Decl. ¶ 7; *see also id.* ¶ 6 (noting that Capital One did not receive ongoing or continuous services from Mandiant under any given SOW). The services Mandiant provided to Capital One during that period were of a different nature entirely, consisting of training and consulting work. *Id.* ¶ 9. *See United States ex rel. Bibby v. Wells Fargo Bank, N.A.*, 165 F. Supp. 3d 1319, 1326 (N.D. Ga. 2015) (distinguishing the "business purpose" of "training to address the issues raised by the investigation" from litigation purposes).[5]

The two cases on which Plaintiffs most heavily rely—*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*, No. 1:19-cv-1050-LMB-MSN, 2019 WL 7592343 (E.D. Va. Dec. 19, 2019)—are inapposite. The *Premera* Court's holding relied on the fact that Mandiant "was performing an ongoing investigation under Premera's supervision ***before outside counsel became involved***" and that Premera had not presented evidence "showing that Mandiant changed the nature of its investigation" after counsel became involved or that its "scope of work and purpose became different in anticipation of litigation." *Id.* at 1245 (emphasis added). In this case,

position would also effectively penalize Capital One for taking the initiative to pre-approve an expert consultant who could readily assist counsel in responding to a cybersecurity incident should one occur.

[5] Further, that Capital One elected to exhaust the retainer it had paid Mandiant under its 2019 SOW before tapping other funds is of no moment. In fact, the majority of the fees paid to Mandiant came from Capital One's legal budget for discovery and investigative costs related to the Cyber Incident, in accordance with the nature of the services Mandiant provided. *See* Watts Decl. ¶ 5.

by contrast, Mandiant performed no work regarding the Cyber Incident until ***after*** Debevoise engaged it to do so. Blevins Decl. ¶ 14; Cantwell Decl. ¶ 6.

Dominion is also distinguishable. First, the court there found that the defendants had not shown that the nature of the work Mandiant was doing for Dominion changed after the breach was discovered and defendants retained counsel. *See* 2019 WL 7592343 at *4. For reasons already noted, the case is distinguishable on that basis alone. Second, more than two months elapsed between Dominion's discovery of the intrusion and its public announcement, during which time Mandiant "concluded its investigation." *See id.* at *2 (noting that Mandiant's investigation on Dominion's behalf concluded by May 17, 2019); *see also Dominion*, Case No. 1:19cv01050-LMB-MSN, Doc. No. 93 at 2 (stating Dominion discovered the intrusion on April 17, 2019 and began notifying customers on June 21, 2019). Critically, the *Dominion* plaintiffs did not file their lawsuit until August 9, 2019, nearly three months after Mandiant finished its investigation, calling into question whether Mandiant's work was even done in anticipation of litigation. Third, there was no evidence in *Dominion* that the fruits of Mandiant's work were used for legal purposes as they were here.

The *Dominion* court also stressed that there was "no evidence of a two-track investigation," meaning the Mandiant report was "the only report commissioned" to investigate the Dominion data breach. 2019 WL 7592343 at *4. But here, Capital One conducted multiple internal investigations after the Cyber Incident. *See* Mot. Ex. 13 at 21-22 (listing multiple internal investigations). Capital One does not categorically claim work product protection or privilege over all of these company-led investigations, and has produced and will produce documents relating to certain of them. Such an approach is consistent with the facts and holdings of *Target* and *Experian*, in which the defendant companies also conducted parallel internal business

investigations alongside the privileged expert investigations the courts held to be protected from disclosure. *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 … in litigation that commenced almost immediately after the breach" was announced); *Experian*, 2017 WL 4325583, at *2 (noting the existence of separate "internal investigation" and "remediation efforts").[6]

B. The Mandiant Report Is Not an Ordinary-Course, Business Document.

Plaintiffs' contention that the Mandiant Report is not protected work product hinges on the argument that it served a "business purpose" and that Capital One had a pre-existing regulatory obligation to commission the Report. Both arguments fail.

1. The Mandiant Report was not commissioned for business purposes.

The contention that Mandiant's post-breach investigation "served a business function unrelated to litigation" (Mot. at 15) is false. If the Mandiant Report had been prepared for business purposes, it would have been widely shared with Capital One's business personnel involved in reviewing and remediating the Incident. But it was not. *Cf. Experian*, 2017 WL 4325583, at *2 (noting that "Mandiant's full report wasn't given to Experian's Incident Response Team"). Not only was Mandiant's work directed and supervised by Debevoise, but once the Mandiant Report was complete, it was delivered first to Debevoise, which then provided it to Capital One's legal department. Cantwell Decl. ¶ 20. Capital One's legal team shared the Mandiant Report with only a limited number of non-legal employees, and the names of all recipients were logged by the legal

[6] As a final point, that some litigants have apparently decided to produce other reports prepared by Mandiant in other cases, *see* Mot. at 10, is entirely irrelevant to determining whether *this* Report is protected by the work product doctrine. As Plaintiffs themselves acknowledge, such determinations "require[] a 'case-by-case' analysis." Mot. at 7.

department. *See* Blevins Dec. ¶¶ 17-18; Ex. 2 at 7-8. Tellingly, only four employees in Capital One's roughly 600-person Cyber Organization received the Mandiant Report. *See* Ex. 2 at 7-8; *see also* Mot. Ex. 3 at -185311, -185312.

Plaintiffs' citation to a *pre*-Cyber Incident slide deck designating other Mandiant-related expenditures as "Business Critical" says nothing about the nature of Mandiant's *post*-Cyber Incident investigation. *See* Mot. at 15. Determining whether a document is protected work product must be done as of the time the document was 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 finding materials created after "Defendant reasonably perceived that the circumstances could result in litigation" to be protected). And the February 2019 document Plaintiffs cite does not concern the fees paid to Mandiant for its work on the Cyber Incident.[7]

In sum, Debevoise did not retain Mandiant to investigate or issue the Report for purposes of Capital One's ordinary business.

2. Capital One's incidental use of the Mandiant Report for business reasons does not change that it was created because of litigation in the first instance.

The Mandiant Report was created because of litigation; that it may have *also* served an incidental business purpose does not strip it of work product protection. Courts have repeatedly recognized that materials prepared in anticipation of litigation may have additional, non-litigation purposes and still retain their protected status. As the D.C. Circuit observed, "material generated in anticipation of litigation may also be used for ordinary business purposes without losing its

[7] Plaintiffs also cite a draft set of investor relations "talking points" referencing Mandiant's retention, claiming it was intended to "reassure[e] outside entities" about the Cyber Incident. Mot. at 18. But not only do Plaintiffs offer no evidence showing that these talking points were ever used, the Company'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.

protected status." *Deloitte*, 610 F.3d at 138. Similarly, the Second Circuit's *Adlman* decision held that "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 influenced by the likely outcome of the anticipated litigation." *United States v. Adlman*, 134 F.3d 1194, 1195 (2d Cir. 1998); *see also In re Grand Jury Subpoena (Mark Torf/Torf Envtl. Mgmt.)*, 357 F.3d 900, 910 (9th Cir. 2004) (holding that "dual purpose" documents—i.e., documents created both in anticipation of litigation and for other business needs—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."); *Wells Fargo*, 165 F. Supp. 3d at 1326 ("This secondary business purpose does not serve to strip the [withheld material] of work product protection.").

Plaintiffs' statement that "the primary purpose of the [Mandiant] investigation was not litigation" is not just wrong, it improperly conflates the Fourth Circuit's standard—under which materials prepared "because of the prospect of litigation" receive protection—with the more restrictive test, adopted only in the Fifth Circuit, requiring litigation to be the "primary motivating purpose" for the materials' creation. *See, e.g.*, *In re El-Atari*, No. 11-01427, 2013 WL 593705, at *6 (E.D. Va. Bankr. Feb. 14, 2013) (describing the Fourth Circuit's "because of" test as "more lenient" than the Fifth Circuit's standard and holding that documents serving a "parallel, non-litigation need" were nonetheless protected by the work product doctrine). In *El-Atari*, the Court aptly observed that to limit work product protection to documents prepared exclusively for litigation—while denying it as to all documents that have any other non-litigation purpose—would mean that "regulated institutions such as banks, which are always required to conduct

investigations into [certain types of wrongdoing] … could never have the protection of the work product doctrine." *Id*.

3. The Mandiant Report was not commissioned to serve a regulatory or compliance-related function.

Plaintiffs also incorrectly contend that Capital One cannot claim work product protection over the Mandiant Report because Capital One, "as a regulated banking entity," had other legal obligations to investigate the Cyber Incident beyond litigation. Mot. at 13. The plaintiffs in *Experian* made precisely the same argument, but the Court rightly rejected it, holding that "Experian indeed had duties under the law to investigate data breaches … [b]ut the record before the Court makes it clear that Mandiant conducted the investigation and prepared its report for Jones Day in anticipation of litigation, *even if that wasn't Mandiant's only purpose*." 2017 WL 4325583, at *2 (emphasis added). The same is true here.

Plaintiffs also mis-rely on *Collins v. Mullins*, in which the court concluded that written statements obtained by a sheriff's office during an internal investigation into police misconduct were not work product. *See* 170 F.R.D. 132, 136 (W.D. Va. 1996). First, the sheriff's office had adopted rules and regulations that not only required it to conduct the investigation but "explicitly mandate[d]" that it prepare written witness statements during the investigation. *Id.* at 135. Here, nothing in the GLBA (*see* Mot. at 13) required Capital One to prepare a written report of its investigation into the Cyber Incident, much less to commission a third party to create such a report. Second, as *Collins* recognized, the "policies that inspire the work product doctrine are wholly inapplicable" to "police departments [that] are under an affirmative duty, in the normal course of serving their public function, to investigate alleged misconduct." 170 F.R.D. at 135. Here, by contrast, Capital One is a private entity, and neither its nor Mandiant's investigation of the Cyber Incident was intended to serve a public function. And, unlike the witness statements in *Collins*,

the Mandiant Report was not prepared in the normal course of business, but with an eye toward litigation.

C. Plaintiffs' Claim that "Facts" Are Not Protected Misses the Mark.

Plaintiffs' repeated refrain is that Mandiant conducted a "factual investigation" and "[t]he underlying facts that Mandiant's investigation discovered are undoubtedly not privileged." Mot. at 3, 11, 21; *see also id.* at 3 (similar).

It is not Capital One's position that historical "facts" or source materials related to the Cyber Incident are protected just because they were observed by Mandiant. The Mandiant Report, though, is not a recitation of "facts," but instead reflects the *opinion* work product of both Mandiant and Capital One's outside counsel. *See* Fed. R. Civ. P. 26(B)(3)(B) (opinion work product consists of the "mental impressions, conclusions, opinions, [and] legal theories of a party's attorney or other representative"); *Nat'l Union*, 967 F.2d at 984 (opinion work product prepared "by the attorney or by another 'representative' of the party" enjoys near absolute protection). In particular, Mandiant used its expertise to identify, draw inferences from, and analyze the underlying technical data, and reached *conclusions* and *interpretations* about that data that it conveyed to Debevoise. *See* Cantwell Decl. ¶¶ 15-17, 19. Mandiant's opinions, moreover, provide the factual foundation for, and cannot be decoupled from, counsel's own theories, impressions, and opinions about the Cyber Incident and related litigation. *See id.*; *U.S. v. Kovel*, 296 F.2d 918, 922 (2d Cir. 1961) (comparing accountant who advised attorney about accounting concepts to foreign language translator). Further, because Mandiant worked at Debevoise's direction, any discussion of the source materials Mandiant reviewed would reveal *counsel's* thought processes and professional judgment about the facts, issues, and defenses Debevoise and Mandiant believed were important to this case. *See In re Allen*, 106 F.3d 582, 608 (4th Cir. 1997) (counsel's selection and

arrangement of documents is opinion work product even if documents themselves are discoverable). In sum, the Mandiant Report is opinion work product and therefore is inviolate.

To the extent the Mandiant Report contains descriptions of purely historical facts, it is nevertheless protected work product. Fact work product consists of any work product that is not opinion work product. *See* Fed. R. Civ. P. 26(b)(3)(A). Both fact and opinion work product "are generally protected and can be discovered only in limited circumstances." *Bridges v. City of Charlotte*, No. No. 3:16-cv-564-GCM, 2017 WL 5715986, at *2 (W.D.N.C. Nov. 28, 2017) (quoting *In re Grand Jury Proceedings, Thursday Special Grand Jury Sept. Term, 1991*, 33 F.3d 342, 348 (4th Cir. 1994)). Summaries, memoranda, and even *pure recitations* of "facts" created in anticipation of litigation have long enjoyed work-product protection. *See Hickman v. Taylor*, 329 U.S. 495, 512 (1947) (written statements attorney obtained from witnesses in anticipation of litigation held protected work product); *see also* Fed. R. Civ. P. 26(b)(3)(A)–(B) (providing qualified privilege for fact work product). Thus, even otherwise discoverable historical facts constitute protected work product when recorded in a separate form by an attorney, an attorney's consultant, or a party in anticipation of litigation. *See Hickman*, 329 U.S. at 512 (written statement signed by witness for attorney was protected even though same facts readily available from witness himself); *Allen*, 106 F.3d at 608 (compilation of employment records selected by counsel during investigation protected, even though underlying employment records were not). Although fact work product may be discovered upon a showing of substantial need and undue hardship, Fed. R. Civ. P. 26(b)(3)(A)(i)–(ii), as explained *infra* at Part III, Plaintiffs have not—and cannot—make that showing.

Put simply, Plaintiffs' argument that "factual investigation[s]" (Mot. at 13) cannot be protected is incorrect. The Federal Rules unambiguously provide that "[d]ocuments and tangible

things that are prepared in anticipation of litigation . . . by or for [a] party or its representative" are protected regardless of whether they concern facts. Fed. R. Civ. P. 26(b)(3)(A).

II. CAPITAL ONE HAS NOT WAIVED WORK PRODUCT PROTECTION OVER THE MANDIANT REPORT.

Plaintiffs incorrectly contend that Capital One waived work product protection over the Mandiant Report by sharing it with its banking regulators and auditors at E&Y and by putting "two of the major findings of the Mandiant Report at issue in this litigation." Mot. at 18–19.[8]

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

The work product rule recognizes that "since an attorney's work is for his client's advantage, opposing counsel or adverse parties should not gain the use of that work through discovery." *In re Doe*, 662 F.2d 1073, 1081 (4th Cir. 1981). Only disclosures that "create[] a substantial risk that [work product] will be received by an adversary waive[] the protection." *Cont'l Cas. Co.*, 537 F. Supp. 2d at 772; *see Sheets v. Ins. Co. of N. Am.*, No. 4:04-cv-00058, 2005 WL 3006670, at *2 (W.D. Va. Nov. 8, 2005) ("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*." (emphasis added)). Here, Capital One did not waive work product protection by disclosing the Mandiant Report to its banking regulators and auditors.

First, the FSRRA explicitly provides that there is no waiver when a financial institution shares privileged or protected material with its banking regulators. *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

[8] Plaintiffs also note Capital One shared the report internally with certain Capital One employees. But Plaintiffs do not contend that such internal sharing amounts to a waiver; nor could they. *See Upjohn Co. v. United States*, 449 U.S. 383, 394 (1981) (corporation's privilege extends to employees).

as waiving, destroying, or otherwise affecting any privileges such person may claim with respect to such information[.]" (emphases added)); *see also* 12 U.S.C. § 1813(z) (defining "Federal banking agency" as the OCC, FRB, and FDIC); *see Ak. Elec. Pension Fund,* 2016 WL 6779901, at *4 (stating submissions of work product to "prudential" regulators would not waive privilege). Capital One's disclosures of the Mandiant Report to its bank regulators thus could not have created a waiver as a matter of federal law.

Independently, Capital One's disclosures to its banking regulators did not result in a waiver because those regulators are not adverse to Capital One. Far from being adversarial, "bank supervision" is "relatively informal and more or less continuous." *In re Subpoena Served Upon Comptroller of Currency, & Sec'y of Bd. of Governors of Fed. Reserve Sys.*, 967 F.2d 630, 634 (D.C. Cir. 1992); *see also Vanguard Sav. & Loan Ass'n v. Banks*, No. 93-cv-4627, 1995 WL 555871, at *5 (E.D. Pa. Sept. 18, 1995) (bank and state banking regulator not adverse during regulatory investigation). Nor did disclosing the report to banking regulators create a significant risk that the Mandiant Report would end up in the hands of Capital One's litigation adversaries—after all, Capital One's communications with its banking regulators are themselves privileged. *See* 12 C.F.R. § 4.36 *et seq*. (OCC); 12 C.F.R. § 261.20 *et seq*. (FRB); 12 C.F.R. § 309.1 *et seq*. (FDIC); 12 C.F.R. § 1070.40 *et seq*. (CFPB); *see also Deloitte*, 610 F.3d at 140 (the question is whether disclosure increases the risk that an adversary *in the litigation* will obtain the material); *In re Doe*, 662 F.2d at 1081.

Finally, Capital One did not waive work product protection by disclosing the Mandiant Report to E&Y. Courts have repeatedly held that a company's disclosure of work product to an auditor does not waive work product protection, reasoning that auditors are not their clients' adversaries (much less in the litigation sense). *See, e.g.*, *Deloitte*, 610 F.3d at 140 (no waiver, and

noting the question is whether "Deloitte could be Dow's adversary in the sort of litigation the [work product addresses]"); *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) (investigative reports disclosed to independent auditor remained protected because the auditor-client relationship is not adversarial in sense contemplated by the work product doctrine). This rule serves the interests of creditors, investors, and other stakeholders—all of whom benefit from auditors having access to documents bearing on material litigation potentially facing their clients. *See Saks, Inc.*, 2006 WL 1564684, at *3.

B. Capital One Did Not Place the Mandiant Report "At Issue."

Plaintiffs contend that Capital One put the Mandiant Report "at issue" by claiming on its website that it "immediately fixed the issue" that led to the Cyber Incident and by stating in an interrogatory response that "it determined that Paige Thompson was the only hacker to exploit the issues that gave rise to the Breach." Mot. at 19 & n.12. But neither of those statements refers or cites to the Mandiant Report or purports to be based on Mandiant's investigation, and Capital One (not Mandiant) verified the answers to Plaintiffs' interrogatories.

More fundamentally, Plaintiffs' position turns the "at issue" waiver doctrine on its head. According to Plaintiffs, because information related to the flaw the hacker exploited might be "addressed in the Mandiant Report," Capital One has put the Mandiant Report "at issue." *Id.* But the "at issue" exception to the work product rule does not work that way. It applies 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. U.S.*,

219 F.R.D. 87, 92 (D. Md. 2003). A party places information directly "at issue" only if the party "makes testimonial use" of the protected information or "selective[ly] disclose[s]" the information for "tactical purposes." *MeadWestvaco v. Rexam PLC*, No. 1:10-cv-511, 2011 WL 2938456, at *5-*6 (E.D. Va. July 18, 2011); *E.I. Dupont*, 269 F.R.D. at 608. The general statements Plaintiffs cite do not reference the Mandiant Report or show any intent on Capital One's part to use the Mandiant Report in this litigation.

III. PLAINTIFFS CAN OBTAIN THE SUBSTANTIAL EQUIVALENT OF THE MANDIANT REPORT THROUGH OTHER MEANS WITHOUT UNDUE HARDSHIP.

The Court should reject Plaintiffs' argument that they "have a substantial need for the [Mandiant] Report and [that] it will be impossible or unduly difficult for Plaintiffs to obtain the same information through other means." Mot. at 21.

As a threshold matter, the Mandiant Report contains Mandiant's *opinions and interpretations* about the circumstances in which the Cyber Incident occurred based on its review and interpretation of historical data. *See* Cantwell Decl. ¶¶ 15-17. As such, it is core, opinion work product that is not subject to disclosure even upon a showing of need. *See* Fed. R. Civ. P. 26(b)(3)(B); *Bridges*, 2017 WL 5715986, at *2 (opinion work product enjoys "nearly absolute immunity") (internal citation omitted).

Moreover, to the extent the Mandiant Report contains any purely factual material, Plaintiffs have no "substantial need" for the information and would suffer no "undue hardship" from having to obtain the "substantial equivalent [of that information] by other means." Fed. R. Civ. P. 26(b)(3)(A)(i)–(ii). Plaintiffs concede as much in their Motion. The basis for their request for the Mandiant Report is not that they are unable to otherwise obtain any facts contained in it, but that compelling Capital One to produce it will "enable Plaintiffs to prosecute their case more efficiently" and "will necessarily streamline the discovery process." Mot. at 21. The work product

doctrine, however, serves as an "'anti-freeloader' rule designed to prohibit one adverse party from riding to court on the enterprise of another," *Nat'l Union*, 967 F.2d at 985, and compelling Capital One to produce the Mandiant Report simply because doing so might make Plaintiffs' job easier would violate that maxim. *See also Hickman*, 329 U.S. at 516 (Jackson, J., concurring) ("Discovery was hardly intended to enable a learned profession to perform its functions . . . on wits borrowed from the adversary.").

Plaintiffs also claim that having to independently "search through thousands of documents and communications – many of which may have no relevance to the Breach at issue – to piece together" facts in the Mandiant Report would impose an "undue hardship." Mot. at 21. But having to use the discovery tools available to them is in no way an "undue hardship." *See Sicurelli v. Jeneric/Pentron Inc.*, No. 03-cv-4934, 2006 WL 1329709, at *3 (E.D.N.Y. May 16, 2006) (denying motion to compel even though "[i]t is true that other discovery devices may be more expensive or burdensome than the production of the protected documents"). After all, Plaintiffs brought these lawsuits, and to the extent Capital One has produced documents to Plaintiffs that are unrelated to the Cyber Incident, it is only because Plaintiffs asked for them.[9]

Ultimately, Plaintiffs have all the discovery devices they need to discover the "facts" Mandiant reviewed during its investigation. And Plaintiffs have used those devices here. *See, e.g.*, Ex. 3, Pls.' First Document Requests at 13, No. 24 (requesting "correspondence, service desk tickets, security architectural reviews, change approvals and change management documents," and other documents "supporting" incident reports concerning the breach); *id.* at No. 28 (requesting

[9] To the extent Plaintiffs contend that reviewing documents they requested that are unrelated to the Cyber Incident gives rise to an undue hardship, it is a crisis of their own making. For that matter, allowing a party to create the very circumstances that give rise to that party's purported need for work product creates perverse incentives in the course of discovery.

"[a]ll event logs prepared or reviewed as part of any investigation of the Breach"); Ex. 4, Pls.' First Interrogs. at 6, No. 9 ("Describe in detail Paige Thompson's creation of . . . credentials and use of those credentials to access Capital One's AWS system[.]"); *id.* at No. 10 ("Identify each location or component of Capital One's AWS cloud on which PII was or may have been accessed during the Breach[, including] the type(s) and amount(s) of accessed data; the file name and size containing the data; the manner by which the unauthorized access was made, and the time period during which such unauthorized access occurred."); *id.* at No. 12 ("Describe in detail any remedial actions undertaken by You, or others acting on Your behalf, relating to the Breach[.]"); *id.* at 7, No. 16 ("Describe in detail whether and how You determined the earliest date that any PII was accessed during the Breach[.]"); Ex. 5, Pls.' Notice of 30(b)(6) Dep. of Capital One (seeking testimony on a wide variety of specific topics relating to the Cyber Incident, including "[w]hen and how the Data Breach . . . occurred;" and "how the information or data was compromised in the Breach").[10]

The Cyber Incident was a discrete event that is reflected in thousands of documents that are not privileged or protected and that have already been, or will be, produced. To the extent the underlying data Debevoise and Mandiant reviewed is responsive to Plaintiffs' discovery requests, it will be disclosed. Further, Plaintiffs' counsel sought leadership positions from the Court based on representations that they had sufficient resources to adequately litigate this case. *See* Dkt. 135 at 3–4; Dkt. 136 at 4; Dkt. 140. They cannot now claim that being asked to use those resources constitutes an undue hardship. *See In re Hardwood P-G, Inc.*, 403 B.R. 445, 466 (Bankr. W.D. Tex. 2009) ("It is not an undue hardship that the defendants have to do their own work.").

[10] Capital One has already agreed to present three corporate representatives in the coming weeks to testify on the majority of topics set out in Plaintiffs' Notice of 30(b)(6) Deposition of Capital One.

Additionally, Plaintiffs have the resources to hire an expert, like Mandiant, to review that data and offer his or her own opinions about the Cyber Incident. *See also* Wright & Miller, Fed. Prac. & Proc. § 2032 ("It must be recalled that the assumption is that ordinarily each party has a full opportunity to retain its own expert; unlike fact witnesses they are not unique[.]"). Capital One has produced (or will produce) the information that would allow Plaintiffs' experts to reach their own conclusions about the data breach at issue in this litigation. *See, e.g.*, *Dale v. Jordan*, No. 2:16-cv-733, 2017 WL 11507179, at *2 (E.D. Va. Nov. 16, 2017) (party could not obtain witness statements prepared by investigator because "[t]he witnesses [were] equally available to [her] or her investigators"). The Court should accordingly deny Plaintiffs' request for the Mandiant Report under Federal Rule of Civil Procedure 26(b)(3)(A).

IV. THERE IS NO BASIS TO COMPEL PRODUCTION OF THE ADDITIONAL COMMUNICATIONS PLAINTIFFS SEEK.

Plaintiffs also ask the Court to compel production of communications between (1) Mandiant and Capital One employees regarding the Cyber Incident and remediation; (2) Capital One employees and third-parties discussing the Mandiant Report and its conclusions; and (3) Capital One employees internally discussing the Mandiant Report, its conclusions and recommendations, and efforts to implement the proposed remediation measures. The Court should deny Plaintiffs' request for three reasons.

First, Plaintiffs' request for additional communications is procedurally improper. Plaintiffs correctly note that the parties have conferred regarding Capital One's assertion of work product protection over the Mandiant Report itself (Mot. at 2), but Plaintiffs have never before challenged Capital One's claim of privilege over those categories of communications or over any

specific communications falling within those categories.[11] Under the Local Rules, "[n]o motion concerning discovery matters may be filed until counsel shall have conferred in person or by telephone to explore with opposing counsel the possibility of resolving *the discovery matters in controversy*." E.D. Va. Loc. Civ. R. 37(E) (emphasis added); *see also id.* (stating the Court "will not consider" a motion concerning discovery matters unless "a good faith effort has been made between counsel to resolve the discovery matters at issue"). Accordingly, only Plaintiffs' request for the Mandiant Report itself is properly before the Court.

Second, as explained earlier, the Mandiant Report is protected work product; Capital One has not waived that protection; and Plaintiffs have not shown a substantial need or undue hardship that warrants setting that protection aside. And because Plaintiffs' *sole basis* for seeking these additional communications is that the Mandiant Report is not protected, the Court should deny their request outright.

Third, even if the Court concludes that the Report is not work product, it does not follow that communications pertaining to the Report or Mandiant's work are not privileged or protected. Whether a particular communication is privileged or is work product is a fact-based analysis that must be performed on a document-by-document basis. *See NLRB v. Interbake Foods, LLC*, 637 F.3d 492, 503 (4th Cir. 2011) ("Generally, each e-mail within a particular line of discussion must be analyzed separately for privilege purposes."). And Plaintiffs' broadside attack on entire categories of communications, without identifying a single communication they believe should be produced, is not a proper way to raise a privilege challenge. *See, e.g.*, Am. Stip. Protective Order

[11] During meet and confers regarding the Mandiant Report, Plaintiffs have requested certain categories of communications that arguably fall within the broader categories their motion seeks to compel (*see* Mot. Ex. 14 at 1). But Plaintiffs have not *challenged* any privilege claims over those narrow categories of communications.

at 23 (setting forth orderly procedure for parties to challenge assertions of privilege on a document-by-document basis). Capital One reviews documents individually for privilege, and all relevant, non-privileged, non-work product communications will be produced, while those that are privileged will be redacted or withheld and logged. Plaintiffs may challenge those determinations in the proper manner, on a document-by-document basis, at the proper time, but their current request is unsupported and premature.

CONCLUSION

For these reasons, the Court should deny Plaintiffs' motion to compel.

Respectfully submitted this 6th day of May, 2020.

/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
Tel.: (404) 572-4600
Fax: (404) 572-5140
dbalser@kslaw.com
shaskins@kslaw.com
jtoro@kslaw.com
kobrien@kslaw.com
rgriest@kslaw.com

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

Counsel for Capital One

CERTIFICATE OF SERVICE

I hereby certify that on May 6, 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