UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

GUO WENGUI, **Plaintiff,** **v.** **CLARK HILL, PLC, *et al.*,** **Defendants.**	**Civil Action No. 19-3195 (JEB)**

MEMORANDUM OPINION

Malicious cyberattacks have unfortunately become a routine part of our modern digital world. So have the lawsuits that follow them, alleging, as this one does, that the hacked institution failed to take sufficient precautions to protect the plaintiff's data. During such litigation, disputes frequently arise over whether documents generated by the defendant in the wake of a data breach — *e.g.*, forensic reports, analyses, and internal communications — are privileged or instead must be turned over in discovery. See, e.g., In re Dominion Dental Servs. USA, Inc. Data Breach Litig., 429 F. Supp. 3d 190, 193–94 (E.D. Va. 2019) (citing cases). This Court now adds its thoughts to the accumulating caselaw.

Plaintiff Guo Wengui has moved to compel Defendant Clark Hill, PLC, his former law firm, to produce "all reports of its forensic investigation into the cyberattack" that led to the public dissemination of Mr. Guo's confidential information. See ECF No. 25-1 (Mot.) at 3; see generally Guo Wengui v. Clark Hill, PLC, 440 F. Supp. 3d 30 (D.D.C. 2020) (discussing Plaintiff's allegations). He also asks that the Court mandate that Defendant provide more complete answers to certain interrogatories regarding its investigation into the hack. See Mot. at 3.

Clark Hill rejoins that it has turned over all relevant internally generated materials and that the other documents Plaintiff seeks, which were produced by external security-consulting firm Duff & Phelps, are covered by both the attorney-client and work-product privileges. See ECF No. 30-1 (Opp.) at 2. The firm points out that it did not hire Duff & Phelps; instead, the consultants were retained by Defendant's outside litigation counsel Musick, Peeler & Garrett to assist in MPG's representation of Clark Hill and to help "prepare for litigation stemming from the attack." Id. The firm also refuses to answer Plaintiff's interrogatories seeking "Clark Hill's understanding of the facts or reasons why" the attack occurred, claiming that "its 'understanding' of the progression of the . . . incident is based solely on the advice of outside counsel and consultants retained by outside counsel" and is therefore privileged. See ECF No. 29-4 (Defendant's Third Supplemental Interrogatory Responses) at 13–14; see also id. at 19 (declining to answer interrogatory regarding effect of attack "to the extent it calls for knowledge that Clark Hill obtained as a result of its consultations with outside counsel and consultants retained by outside counsel").

Separately, Clark Hill also maintains that it cannot respond to Guo's additional requests for "information or documents related to [its] clients other than Plaintiff" who may (or may not) have been affected by the hack at issue, on the grounds that such information is both irrelevant and privileged. See Opp. at 22–24.

For the reasons that follow, the Court finds that the Duff & Phelps Report and associated materials are neither protected work product nor attorney-client privileged. It also concludes that Clark Hill must provide the documents requested by Plaintiff regarding the cyberattack's effect on other firm clients, subject to appropriate redactions. The Court, accordingly, will grant Plaintiff's Motion to Compel.

I. Legal Standard

Rule 37 of the Federal Rules of Civil Procedure entitles parties to "move for an order compelling an answer [or] production" if, among other things, "a party fails to answer an interrogatory submitted under Rule 33" or "fails to produce documents . . . requested under Rule 34." Both interrogatories under Rule 33 and document requests under Rule 34 "may relate to any matter that may be inquired into under Rule 26(b)." Fed. R. Civ. P. 33(a)(2); see Fed. R. Civ. P. 34(a) ("A party may serve on any other party a request within the scope of Rule 26(b) . . . ."). Rule 26(b)(1), in turn, sets the "scope of discovery . . . as follows: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case." The main question here is whether material concerning the "matter" that Plaintiff has requested in discovery is privileged under either the work-product doctrine or the attorney-client privilege. For both, the party seeking to withhold a document — here, Clark Hill — bears the burden of showing that the privilege applies. See FTC v. TRW, Inc., 628 F.2d 207, 213 (D.C. Cir. 1980) (attorney-client privilege); United States v. ISS Marine Servs., Inc., 905 F. Supp. 2d 121, 134 (D.D.C. 2012) (work-product privilege).

II. Analysis

The Court first addresses the Duff & Phelps Report under each of the two privileges; it then analyzes whether Clark Hill must turn over documents related to the cyberattack's effect on its other clients.

A. Duff & Phelps Report

1. *Work-Product Privilege*

Rule 26 codifies what is known as the work-product privilege, under which, "[o]rdinarily, a party may not discover documents and tangible things that are prepared in anticipation of

litigation . . . by or for another party or its representative (including the other party's attorney, consultant, . . . or agent)." Fed R. Civ. P. 26(b)(3)(A). To determine whether a document was "prepared in anticipation of litigation," courts in this circuit apply the "because of" test, asking "whether, in light of the nature of the document and the factual situation in the particular case, the document can fairly be said to have been prepared or obtained because of the prospect of litigation." United States v. Deloitte LLP, 610 F.3d 129, 137 (D.C. Cir. 2010) (emphasis added) (citation omitted). "Where a document would have been created 'in substantially similar form' regardless of the litigation," it fails that test, meaning that "work product protection is not available." FTC v. Boehringer Ingelheim Pharms., Inc., 778 F.3d 142, 149 (D.C. Cir. 2015) (quoting Deloitte, 610 F.3d at 138). For that reason, "the privilege has no applicability to documents prepared by lawyers in the ordinary course of business or for other nonlitigation purposes." In re Sealed Case, 146 F.3d 881, 887 (D.C. Cir. 1998) (citation and internal quotation marks omitted); see also Banneker Ventures, LLC v. Graham, 253 F. Supp. 3d 64, 72 (D.D.C. 2017) ("Documents that would have been created in the ordinary course of business irrespective of litigation are not protected by the work-product doctrine.") (cleaned up); United States v. Adlman, 134 F.3d 1194, 1204 (2d Cir. 1998) ("If the district court concludes that substantially the same [document] would have been prepared in any event — as part of the ordinary course of business . . . — then the court should conclude [it] was not prepared because of . . . litigation.").

In light of the record before the Court, including the Duff & Phelps Report itself (which the Court has reviewed *in camera*), Clark Hill has not met its burden to show that the Report, or a substantially similar document, "would [not] have been created in the ordinary course of business irrespective of litigation." Banneker Ventures, 253 F. Supp. 3d at 72. For many organizations, surely among them law firms that handle sensitive materials, "discovering how [a

cyber] breach occurred [is] a necessary business function regardless of litigation or regulatory inquiries. [There is a] need[] to conduct an investigation . . . in order to figure out the problem that allowed the breach to occur so that [the organization] [can] solve that problem and ensure such a breach [cannot] happen again." Dominion Dental, 429 F. Supp. 3d at 193 (quoting In re Premera Blue Cross Customer Data Sec. Breach Litig. (Premera I), 296 F. Supp. 3d 1230, 1245–46 (D. Or. 2017)). It is therefore more likely than not, if not "highly likely[,] that [Clark Hill] would have conducted [an] investigation" into the attack's cause, nature, and effect "irrespective of the prospect of litigation." ISS Marine Servs., 905 F. Supp. 2d at 137. From the Court's *in camera* review, it is clear that the Duff & Phelps Report summarizes the findings of such an investigation, and that "substantially the same [document] would have been prepared in any event . . . as part of the ordinary course of [Defendant's] business." Adlman, 134 F.3d at 1204.

Defendant, notably, does not seem to quarrel with this general thesis. Instead, it offers a more nuanced position, arguing that the Report qualifies as being prepared in anticipation of litigation because it was the result of only one half of a "two-tracked investigation of the incident." Opp. at 2. On one track, Clark Hill's usual cybersecurity vendor, called eSentire, worked "to investigate and remediate the attack" so as to preserve "business continuity." Id.; see also id. at 5 ("Over the . . . several weeks [after the attack], Clark Hill engaged with . . . eSentire . . . to ascertain the nature and remediate the effects of the attack."). Clark Hill points out that it has disclosed documents related to eSentire's work. Id. at 2. On a "separate track from the eSentire work," Defendant insists, was Duff & Phelps, retained by MPG "for the sole purpose of assisting [the firm] in gathering information necessary to render timely legal advice." ECF No. 29-17 (Engagement Letter from MPG) at 1; see also ECF No. 29-16 (Engagement Letter from Duff & Phelps) at ECF p. 1.

In other words, Clark Hill claims, citing In re Target Corp. Customer Data Sec. Breach Litig., MDL No. 14-2522, 2015 WL 6777384, at *2–3 (D. Minn. Oct. 23, 2015), that it had one "ordinary-course investigation" by eSentire "set up so that [it] could learn how the breach happened and . . . respond to it appropriately" — which did not result in protected work product — while it also engaged a "separate team" to "inform[] [its] counsel about the breach so that [they] could provide . . . legal advice and prepare to defend the company in litigation." Id. (finding "information generated along [the latter] track" to be protected work product). Under the Target court's approach, the latter investigation and report would apparently not have existed but for the prospect of litigation, even as the other report would have been prepared "in the ordinary course of business." In re Sealed Case, 146 F.3d at 887 (citation omitted). Ergo, says Clark Hill, it has appropriately disclosed eSentire's work and held on to Duff & Phelps's.

The problem for the defense here is that its two-track story finds little support in the record. The firm offers no sworn statement averring that eSentire conducted a separate "investigation" with the purpose of "learn[ing] how the breach happened" or facilitating an "appropriate[]" response. Target, 2015 WL 6777384, at *2. The closest it comes is an equivocal statement by Eric Rouseau, its Director of Information Security, that "[b]ecause of eSentire's work, Clark Hill did not need the Duff & Phelps report for business continuity." ECF No. 29-29 (Declaration of Eric Rouseau), ¶ 4. That is not the same as stating that eSentire conducted its own inquiry to (in the words of Defendant's brief) help Clark Hill "ascertain the nature and remediate the effects of the attack." Opp. at 5. On the contrary, Defendant's own interrogatory answers state that "its understanding of the progression of the September 12, 2017 cyber-incident is based solely on the advice of outside counsel and consultants retained by outside counsel." Def.'s 3d Suppl. Interrog. Resps. at 13–14 (emphasis added) (internal quotation marks omitted);

see also ECF No. 25-6 (Defendant's Second Supplemental Interrogatory Responses) at 17–18 (earlier interrogatory answer stating that "any belief held by Clark Hill regarding the cause or origination of the cyber-incident is the result of discussions with outside counsel and consultants retained by outside counsel") (emphasis added). Consistent with those answers, there is no evidence that eSentire ever produced any findings, let alone a comprehensive report like the one produced by Duff & Phelps, about "the problem that allowed the breach to occur" or any recommendations to "ensure such a breach [cannot] happen again." In re Premera Blue Cross Customer Data Sec. Breach Litig. (Premera II), 329 F.R.D. 656, 666 (D. Or. 2019); see also Premera I, 296 F.3d at 1245 ("This situation is unlike the Target data breach case . . . . [There,] the company performed its own independent data breach investigation that was produced in discovery.") (emphasis added); Dominion Dental, 429 F. Supp. 3d at 195 ("Here, defendants have presented no evidence of a two-track investigation. The . . . report [at issue] appears to be the only report commissioned by defendants in connection with the data breach at issue.").

The record instead suggests that on September 14, 2017, two days after the cyberattack began, Clark Hill turned to Duff & Phelps instead of, rather than separate from or in addition to, eSentire, to do the necessary investigative work. The firm has pointed to no documents reflecting eSentire's doing investigative or remedial work after September 14, even though, from all indications, the attack was potentially still ongoing and the firm did not yet have a full understanding of its cause or scope. See ECF No. 38-1 at ECF p. 1 (September 13 email from eSentire providing "not necessarily complete" timeline of attack and noting that network "may be compromised"); ECF No. 38 (eSentire-produced "Event Timeline" showing potential suspicious activity continuing on September 14); ECF No. 25-3 at 1 (letter from Clark Hill's General Counsel dated September 19 stating that firm's "investigation regarding the nature and

extent of the cyberattack [was] continuing"). And at precisely the time the "trail essentially goes cold" as to eSentire's work, see ECF No. 33 (Reply) at 10, Duff & Phelps's began: Rouseau reported that at 1:30 p.m. on the 14th, he "[s]poke with Duff and Phelps to request help with incident" and that the "Duff and Phelps team arrive[d] on-site and beg[an] investigation" at 11:45 p.m. that evening. See ECF No. 38 at ECF p. 3. Internal emails also show that Rouseau and Clark Hill's General Counsel, Edward Hood, held a call the morning of the 15th with Duff & Phelps employees, referring to them as "the incident response team." ECF No. 41-1 at ECF p. 2. The Report confirms this timeline of Duff & Phelps's involvement.

There is more. Hood himself admits that the Report was shared not just with outside and in-house counsel, but also with "select members of Clark Hill's leadership and IT team." Opp. at 6 (citing ECF No. 29-27 (Declaration of Edward J. Hood), ¶¶ 5–6). Hood further avers that the Report was used to "assist[] [Clark Hill] in connection with managing any issues, including" — but notably not limited to — "potential litigation . . . related to the . . . cyber incident." Hood Decl., ¶ 6 (emphasis added). Defendant also shared the report with the FBI "as part of the FBI's investigation of the cyber incident." Id. The Report was probably shared this widely, as Plaintiffs persuasively argue, because it "was the one place where [Defendant] recorded the facts" of what had transpired. See Reply at 10. There was no comparable eSentire document. The Report itself, moreover, reveals yet other ways in which Duff & Phelps worked with persons beyond MPG or Clark Hill to help the firm respond to and manage the breach.

The fact that "the [R]eport was used for a range of non-litigation purposes" reinforces the notion that it cannot be fairly described as prepared in anticipation of litigation. Dominion Dental, 429 F. Supp. 3d at 194; compare id. at 195 ("[I]n Experian, the full report was withheld from defendants' incident response team. Here, defendants have not represented that the full

report was withheld from them."), with In re Experian Data Breach Litig., No. 15-1592, 2017 WL 4325583, at *2 (C.D. Cal. May 18, 2017) (concluding forensic report was work product) ("If the report was more relevant to Experian's internal investigation or remediation efforts, as opposed to being relevant to defense of this litigation, then the full report would have been given to that team."); see also In re Capital One Consumer Data Sec. Breach Litig., No. 19-2915, 2020 WL 2731238, at *5 (E.D. Va. May 26, 2020) (rejecting work-product protection for forensic report "used by Capital One for various business and regulatory purposes"), aff'd, No. 19-2915, 2020 WL 3470261 (E.D. Va. June 25, 2020).

In sum, although engagement letters dated September 14 state that Clark Hill hired MPG in anticipation of litigation and that, on the same day, MPG in turn retained Duff & Phelps, Duff & Phelps's role seems to have been far broader than merely assisting outside counsel in preparation for litigation. Although Clark Hill papered the arrangement using its attorneys, that approach "appears to [have been] designed to help shield material from disclosure" and is not sufficient in itself to provide work-product protection. Dominion Dental, 429 F. Supp. 3d at 194 (finding defendant's "conclusory statement" in affidavit that report was prepared in anticipation of litigation "rebutted by extensive evidence in the record"); Premera II, 329 F.R.D. 656, 666 (D. Or. 2019) (concluding that defendant "cannot shield [consultant forensic work] from discovery by delegating [its] supervision to counsel"); see also Allied Irish Banks v. Bank of Am., N.A., 240 F.R.D. 96, 99 (S.D.N.Y. 2007) ("That [the plaintiff] hired a law firm to 'assist' in the investigation is of no moment. . . . A party may not insulate itself from discovery by hiring an attorney to conduct an investigation that otherwise would not be accorded work product protection.") (cleaned up).

At a minimum, it is Clark Hill's burden to demonstrate that a substantially similar document to the Duff & Phelps Report would not have been produced in the absence of litigation, and it has fallen well short of doing so. Both the Report and related materials (referred to by Defendant as "Expert Materials," Opp. at 11) are accordingly not protected work product.

2. *Attorney-Client Privilege*

Distinct from the work-product privilege, the attorney-client privilege protects "a confidential communication between attorney and client if that communication was made for the purpose of obtaining or providing legal advice to the client." In re Kellogg Brown & Root, Inc., 756 F.3d 754, 757 (D.C. Cir. 2014). The Duff & Phelps Report does not exactly fit within that canonical formulation, as it is not a communication between an attorney and a client, but rather one between an attorney and an outside consultant hired by the attorney. See In re Sealed Case, 676 F.2d 793, 809 (D.C. Cir. 1982) (stating that generally, "communications that do not involve both attorney and client . . . are unprotected"). Although Defendant is not explicit, its unstated argument seems clear enough: the privilege also "can attach to reports of third parties made at the request of the attorney or the client where the purpose of the report was to put in usable form information obtained from the client." TRW, 628 F.2d at 212 (citing United States v. Kovel, 296 F.2d 918 (2d Cir. 1961)). The classic example is a report by an accountant who, like a translator, takes the client's tax or financial information and makes it digestible to the attorney. Id. Clark Hill's argument, then, is that the Duff & Phelps Report qualifies as privileged per this doctrine.

It does not. As the Circuit has explained, the Kovel doctrine must be applied narrowly "lest the privilege be construed to engulf 'all manner of services' that should not be summarily excluded from the adversary process." Linde Thomson Langworthy Kohn & Van Dyke, P.C. v. Resolution Tr. Corp., 5 F.3d 1508, 1514–15 (D.C. Cir. 1993) (quoting TRW, 628 F.2d at 212);

see also In re Lindsey, 158 F.3d 1263, 1272 (D.C. Cir. 1998) ("The attorney-client privilege must be strictly confined within the narrowest possible limits consistent with the logic of its principle.") (cleaned up). After all, unlike the work-product privilege, which may be overcome by a sufficient showing of need, the attorney-client privilege is absolute. To that end, the Kovel court itself made clear that, for instance, "if the advice sought [by the client] is the accountant's rather than the lawyer's, no privilege exists" over the accountant's report. Kovel, 296 F.2d at 922; see also TRW, 628 F.2d at 212 (same).

From the factual record discussed above and the Report itself, the Court concludes that Clark Hill's true objective was gleaning Duff & Phelps's expertise in cybersecurity, not in "obtaining legal advice from [its] lawyer." Linde Thompson, 5 F.3d at 1514 (quoting TRW, 628 F.2d at 212). At a minimum, Defendant has not demonstrated that the opposite is true. Duff & Phelps undertook a full investigation — the only one apparently commissioned by Clark Hill — with the goal of determining how the attack happened and what information was exfiltrated. The Report provides not only a summary of the firm's findings, but also pages of specific recommendations on how Clark Hill should tighten its cybersecurity. And it was shared with both Clark Hill IT staff and the FBI, presumably with an eye toward facilitating both entities' further efforts at investigation and remediation. (Because the Court finds the Report not subject to attorney-client privilege, it does not address Plaintiff's separate argument that Defendant waived the privilege by disclosing the Report to the FBI. See Reply at 17–21.)

The firm points to only one case, the Target decision, that has applied the attorney-client privilege to a similar forensic report, and that non-binding decision (even assuming it is correct) is distinguishable in at least three ways. First, as discussed above, Target had a two-track approach, with one track a concededly "non-privileged investigation . . . . set up so that Target

. . . could learn how the breach happened and . . . respond to it appropriately." 2015 WL 6777384, at *2. Assuming that investigation was sufficient for Target's business purposes, it is much easier to view the other as aimed at facilitating effective legal representation. Second, and relatedly, there is no indication that the Target report was shared as widely for non-legal purposes as the Duff & Phelps Report. Third, the Target court specifically noted that the relevant investigation and report were not "focused . . . on remediation of the breach." Id. at *3. Here, Duff & Phelps was apparently engaged for immediate "incident response" and began its work as the attack was thought to still be ongoing. Its Report, moreover, includes pages of specific remediation advice.

For the foregoing reasons, the Duff & Phelps Report and associated materials are not privileged and must be disclosed, and the related interrogatories must be answered.

B. Other Clark Hill Clients

Defendant separately resists Plaintiff's discovery requests for information relating to the effect of the cyberattack on firm clients other than Guo himself. See Opp. at 22–24. For instance, Plaintiff has served a request for production seeking "[a]ll documents reflecting that the 'hacking' . . . resulted in a third party's obtaining . . . information, data, or material regarding any Clark Hill client other than or in addition to plaintiff." ECF No. 29-18 (March 11 RFP), ¶ 18. Clark Hill claims that this sort of information is both irrelevant and privileged. See Opp. at 22–23. Here, too, the Court will grant Plaintiff's Motion to Compel: the information is clearly relevant, and appropriate redactions can assuage any privilege or privacy concerns.

As to relevance, the scope of the attack is directly germane to a central issue in the case — namely, in Defendant's own words, "the sufficiency and reasonableness of Clark Hill's cybersecurity in September 2017." Id. at 23. One easily conjured example: if the attack was

largely focused on Plaintiff, that might suggest that a reasonable custodian of his documents should have been aware that he in particular was a target and should thus have taken appropriate special precautions. If the attack, conversely, was more of a fishing expedition aimed at a wide swath of the firm's closely held information, that might suggest the opposite. Or perhaps, if the attack was indeed broad, one could argue that a reasonably prudent custodian should have detected it sooner. In short, the sort of information Plaintiff seeks is directly relevant; and even if it were not, there is a "reasonable likelihood that allowing discovery of the[se] documents will lead to discovery of [other] evidence [that is] relevant," which renders them discoverable under Rule 26. Food Lion, Inc. v. United Food & Commercial Workers Int'l Union, AFL-CIO-CLC, 103 F.3d 1007, 1013 (D.C. Cir. 1997).

The firm also contends that it cannot fully answer interrogatories or turn over documents relating to the hack's effect on its other clients because doing so would reveal that it represents those individuals, and the fact of representation itself is attorney-client privileged. See Opp. at 3, 24. That does not quite state the law accurately. As this Court has previously explained, "Under the general rule, the attorney-client privilege does not protect from disclosure the identity of the client . . . and the general purpose of the work performed." Cause of Action Inst. v. U.S. Dep't of Justice, 330 F. Supp. 3d 336, 350 (D.D.C. 2018) (citation and internal quotation marks omitted). On the other hand, "when a client's identity is sufficiently intertwined with the client's confidences," the privilege does apply. Id. (cleaned up and citations omitted). At this point, Defendant (which bears the burden to demonstrate that the privilege applies) has given the Court no way of knowing whether the latter situation is applicable to any documents at issue.

That said, however, privilege is not the only consideration here. Discovery must be both "relevant" and "proportional to the needs of the case," Fed. R. Civ. P. 26(b)(1), and the Court

doubts that the precise identity of any Clark Hill client is relevant to the issues here. To the extent that it is, its germaneness is likely weak enough to be outweighed by the clients' privacy interests. See Henson v. Turn, Inc., No. 15-1497, 2018 WL 5281629, at *5 (N.D. Cal. Oct. 22, 2018) ("Courts and commentators have recognized that privacy interests can be a consideration in evaluating proportionality . . . ."). It thus seems to the Court that Defendant can fully safeguard the identity of its clients and any of their confidences, if applicable, with appropriate redactions in responsive documents and with tailored interrogatory answers. There is no basis, however, for its blanket refusal to respond to Plaintiff's requests for production, and the Court will grant the Motion to Compel that discovery subject to appropriate redactions.

III. Conclusion

For the foregoing reasons, the Court will grant Plaintiff's Motion to Compel. A contemporaneous Order so stating will issue this day.

/s/ *James E. Boasberg*
JAMES E. BOASBERG
United States District Judge

Date: January 12, 2021