ALSTON & BIRD

Privacy, Cyber & Data Strategy

Potential Solutions for Maintaining Attorney-Client Privilege and Work Product Protections over Forensic Reports in Light of *Wengui v. Clark Hill*

February 26, 2021

ALSTON & BIRD

Potential Solutions for Maintaining Attorney-Client Privilege and Work Product Protections over Forensic Reports in Light of *Wengui v. Clark Hill*

By Kim Peretti, Jon Knight, and Emily Poole

* * * * * *

On January 12, 2021, a U.S. district judge for the District of Columbia issued an opinion in *Wengui v. Clark Hill, PLC*[1] granting the plaintiff's motion to compel production of a data breach forensic report and other materials prepared by a third-party forensic consultant. The court ordered production of the forensic report even though the consultant was operating under the direction and control of outside counsel and under an agreement entered into after the discovery of the underlying data breach. The court found that Clark Hill had not established that the forensic report was protected from production by either the attorney-client privilege or work product doctrine, noting that Clark Hill's understanding of the incident seemed to be based solely on the forensic consultant investigation, which would have occurred in the ordinary course of business, and Clark Hill's purpose in hiring the forensic consultant was to obtain cybersecurity expertise, not legal advice.

The *Clark Hill* opinion is notable because not only does it follow a string of recent opinions that have found data breach forensic reports not to be entitled to work product protection,[2] it also goes one step further to find that a data breach forensic report is not protected by attorney-client privilege. In this instance, the court applied a narrow interpretation of the *Kovel* doctrine and found that the company's *true objective* in engaging the forensic firm (that produced the report) was to obtain cybersecurity expertise, not legal advice.

The following is a summary of the *Clark Hill* opinion followed by some considerations for companies seeking to apply the lessons of the opinion to future data breach investigations, including the importance of (1) drawing clear lines between ordinary-course investigations to solely understand the nature and scope of the incident and an investigation for legal purposes; and (2) carefully considering the scope, purpose, and audience of any third-party written reports prepared at the direction of counsel. We conclude with suggested best practices for protecting attorney-client privilege and the work product doctrine during the investigation of a security incident.

---

[1] *Wengui v. Clark Hill, PLC*, No. 1:19-cv-03195 (D.D.C. Jan 12, 2021) ("Mem. Op.").

[2] *See In re Capital One Consumer Data Sec. Breach Litig.*, No. 1:19-md-02915 (AJT/JFA), 2020 U.S. Dist. LEXIS 91736 (E.D. Va. May 26, 2020); *In Re Premera Blue Cross Customer Data Sec. Breach Litig.*, 296 F. Supp. 3d 1230 (D. Or. 2017); *In re Dominion Dental Servs.* United States, 429 F. Supp. 3d 190 (E.D. Va. 2019).

Part One: The Background for the Motion to Compel

Plaintiff Guo Wengui is a Chinese dissident who hired Clark Hill to represent him as he applied for asylum in the United States.[3] Clark Hill was hacked shortly after being engaged by Wengui, in what was allegedly a targeted attack by the Chinese government, and Wengui's asylum application was disclosed online.[4] Clark Hill ended its engagement with Wengui following the cyber-attack, citing considerations under the Rules of Professional Conduct.[5] Wengui then filed suit against Clark Hill, alleging breach of fiduciary duty, breach of contract, and negligence.[6] Among other allegations, he alleges that the cyber-attack demonstrates that Clark Hill did not adequately protect his information.[7]

The plaintiff moved to compel Clark Hill to produce "all reports of its forensic investigation into the cyberattack" that led to the disclosure of his information, including the forensic report.[8] Clark Hill maintains that it turned over all relevant internally generated materials and that the other documents sought by the plaintiff produced by the forensic consultant are covered by both the attorney-client privilege and work product doctrine.[9] Clark Hill also declined to answer the plaintiff's interrogatories seeking "Clark Hill's understanding of the facts or reasons why" the attack occurred, arguing that its understanding of the incident was based on the advice of outside counsel and consultants retained by outside counsel, and is therefore privileged.[10]

The plaintiff raised several arguments in support of his motion to compel, including:

(1) Clark Hill is engaged in "mass withholding" of all information concerning the cyber-attack.

(2) The attorney work product doctrine confers no protection on Clark Hill's forensic investigation of the cyber-attack because Clark Hill would have investigated the cyber-attack even if it were at no risk of being sued.

(3) The forensic consultant report is not attorney-client privileged because Clark Hill's "primary purpose" was not to obtain a legal opinion, and Clark Hill cannot persuade the court that it would not have investigated the cyber-attack at all "but for" its seeking of legal advice.

(4) Clark Hill should not be allowed to avoid its obligations to disclose underlying facts by communicating them to an attorney or having an attorney direct the investigation.

(5) Clark Hill has waived its narrower claim of privilege with the forensic consultant report, particularly because it has failed to particularize its claims of privilege by providing a privilege log.

---

[3] *Wengui v. Clark Hill, PLC*, 440 F. Supp. 3d 30, 33-34 (D.D.C. 2020).
[4] *Id.* at 34.
[5] *Id.* at 34-35.
[6] *Id.* at 35.
[7] *Id.* at 38.
[8] Mem. Op. at 1-2.
[9] *Id.* at 2.
[10] *Id.*

After briefing, the court concluded that the forensic consultant report was not work product and not attorney-client privileged and ordered its production.[11]

Part Two: The Court Finds That the Report Is Not Protected Work Product

The court found that Clark Hill had not met its burden of showing that the forensic consultant report would not have been created in the ordinary course of business, irrespective of litigation, and therefore the court found that the report is not protected work product.

A. The court applied the "because of" test for the work product doctrine.

In assessing whether the forensic consultant report is protected work product, the court applied the "because of" test, asking whether the document in question can fairly be said to have been prepared or obtained *because of* the prospect of litigation.[12] The court wrote that if 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."[13] Citing to *Dominion Dental,* a recent case regarding work product in the context of data breach investigations, the court wrote that discovering how a cyber-attack occurred is a normal business function that would take place regardless of litigation or regulatory inquiries,[14] and therefore the court focused on the specific structure of Clark Hill's data breach investigation and the role of the forensic consultant report as part of Clark Hill's investigatory efforts.[15]

B. The court disagreed with the notion that Clark Hill's investigation was a "two-tracked" investigation, where one track only took place because of the prospect of litigation.

Clark Hill argued that it had a "two-tracked" investigation, similar to Target's investigation of its 2013 data breach, and that the 2015 *Target* decision is precisely on point. In 2015, as part of the Target data breach litigation, the District of Minnesota found that unlike materials produced by Target in discovery that were prepared in connection with Target's ordinary course investigation of the breach with the assistance of a third party, documents prepared in connection with the investigation performed by the third party hired by Target's outside counsel were privileged and protected from discovery.[16] Clark Hill argued that its investigations followed the same two-tracked structure, where one track's investigation was performed in the ordinary course of business, and the other track's investigation was to gather information

---

[11] *Id.* at 18.
[12] *Id.* at 5 (citing *United States v. Deloitte LLP*, 610 F.3d 129, 137, 391 U.S. App. D.C. 318 (D.C. Cir. 2010)).
[13] *Id.* at 5 (citing *FTC v. Boehringer Ingelheim Pharms., Inc.*, 778 F.3d 142, 149, 414 U.S. App. D.C. 188 (D.C. Cir. 2015)).
[14] *Id.* at 6.
[15] Several recent privilege cases, including *Dominion Dental* and *Capital One,* focused on the preexisting relationship between the party requesting the investigation and the third party performing it when finding there was no work product protection for the reports. Here, Clark Hill argued it has work product protection because it had no prior relationship with the forensic consultant and the engagement letter demonstrates that the consultant was retained for the purpose of assisting counsel in rendering legal advice. The court did not focus on this as a distinguishing factor in its analysis.
[16] Response to Motion to Compel, at 12.

necessary to render timely legal advice and prepare for litigation.[17] On the first track, Clark Hill argued that its usual cybersecurity vendor, eSentire, worked with its internal IT team to investigate and remediate the attack, while on a different track, Clark Hill's outside counsel, Musick, Peeler & Garrett (MPG), hired the forensic consultant for the sole purpose of assisting MPG.[18]

The court did not find Clark Hill's two-track argument to be persuasive, instead finding that the investigation was really only one track: the investigation conducted by the forensic consultant.[19] The court noted that Clark Hill offered very little to show that eSentire conducted a separate investigation with the purpose of learning how the breach occurred.[20] Unlike in *Target*, the court found that there is "no evidence that eSentire ever produced any findings," let alone a comprehensive report (even though the court recognized that eSentire produced an "Event Timeline" at one stage of the investigation).[21] Instead, the court found it determinative that Clark Hill's own interrogatory answers state 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 therefore "any such understanding is privileged."[22] As support for the notion that there was no comparable eSentire document, the court highlights that the forensic consultant report was shared not just with outside and in-house counsel, it was shared with select members of Clark Hill's leadership and IT team, and it was used to assist Clark Hill in managing *any* issues arising from the breach (not just litigation).[23]

The court therefore concluded that the report was not protected work product because Clark Hill had not met its burden of demonstrating that a substantially similar document to the forensic consultant report would not have been produced "but for" the prospect of litigation.[24] The court found that the consultant's role seems to have been far broader than merely assisting outside counsel in preparation for litigation and that Clark Hill's approach was designed more to help shield material from disclosure.[25]

Part Three: Clark Hill's "True Objective"

The court found that Clark Hill's "true objective" in hiring the forensic consultant was gleaning the consultant's expertise in cybersecurity – not obtaining legal advice – and therefore the court found that the report is not protected by the attorney-client privilege. As set out below, in reaching this conclusion, the court applied a narrow version of the *Kovel* doctrine and did not

[17] Mem. Op. at 5, 7.
[18] *Id.* at 7-8.
[19] *Id.* at 8-9.
[20] *Id.*
[21] *Id.* at 10-11.
[22] *Id.* at 9.
[23] *Id.* at 12-13.
[24] *Id.* at 14.
[25] *Id.* at 13.

address whether obtaining legal advice must be *the only* or *the primary* purpose of a privileged communication.

A. The court narrowly applied the *Kovel* doctrine.

In assessing whether the forensic consultant report is protected by the attorney-client privilege, the court applied a narrow reading of the *Kovel* doctrine.[26] The court wrote that under the attorney-client privilege, a confidential communication between attorney and client is protected "if that communication was made for the purpose of obtaining or providing legal advice to the client."[27] When the communication is between an attorney and an outside consultant hired by the attorney, the court writes, the *Kovel* doctrine may protect reports "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."[28] The court gives the example of an accountant who takes the client's complex financial information and makes it digestible to an attorney.[29] The court writes that the *Kovel* doctrine must be applied narrowly so that it is not used to shield all manner of services from the discovery process.[30] To that end, the court writes that "if the advice sought [by the client] is the accountant's rather than the lawyer's, no privilege exists" over the accountant's report.[31]

Applying a narrow reading of *Kovel* to the forensic consultant report, the court found that Clark Hill's "true objective" was gleaning the consultant's expertise in cybersecurity, not in obtaining legal advice, and therefore the report is not protected by the attorney-client privilege.[32] The court writes that the report provides not only a summary of the firm's findings but also pages of recommendations on how Clark Hill should tighten its cybersecurity, indicating that the scope of the report was not limited to the immediate impact of the data breach.[33] Moreover, the court found that the report was shared with IT staff and the FBI, apparently for non-legal purposes, further underscoring that the purpose of the report was broader than just providing legal advice.[34]

B. The court sidesteps the parties' arguments about whether obtaining legal advice must be the only or primary purpose of a privileged communication.

Interestingly, although the parties disagree on the proper test in the D.C. Circuit for whether a communication is privileged, the court spends very little time on this issue, leaving questions around whether obtaining legal advice must be *the only* or *the only significant* purpose of a privileged communication.

---

[26] *See United States v. Kovel*, 296 F.2d 918 (2d Cir. 1961).
[27] Mem. Op. at 14 (citing *In re Kellogg Brown & Root Inc.*, 756 F.3d 754, 757, 410 U.S. App. D.C. 382 (D.C. Cir. 2014)).
[28] *Id.* at 15 (citing *Kovel*).
[29] *Id.* at 15.
[30] *Id.* at 15.
[31] *Id.* at 16 (citing *Kovel*).
[32] *Id.* at 16.
[33] *Id.*
[34] *Id.* The plaintiff also argued that since Clark Hill had disclosed the report to the FBI, it had also waived any claim of attorney-client privilege over the report. The court did not rule on the waiver issue since it found the report was not protected by privilege in the first instance. Mem. Op. at 11.

The plaintiff argues that the test for privilege has two parts: (1) whether the "primary purpose" of the communication is to obtain a legal opinion, legal services, or assistance in a legal proceeding; and (2) whether the communication would not have been made "but for" the fact that legal advice was sought.[35] The plaintiff argues that therefore Clark Hill "must persuade the court that, 'but for' the fact that it sought legal advice from [MPG], it would have done nothing – literally, nothing – in response" to the data breach.[36]

Clark Hill argues, on the other hand, that the plaintiff erroneously applied privilege case law by applying the but-for test for attorney-client privilege instead of the "significant purpose" test.[37] Clark Hill cites to *In re Kellogg Brown & Root, Inc.*, the same case cited by the district court in its opinion, arguing that in that case, the D.C. Circuit explained that the but-for test was not the appropriate test for attorney-client privilege analysis.[38] Clark Hill writes that instead, the D.C. Circuit found that "[s]o long as obtaining or providing legal advice was *one of the significant purposes* of the internal investigation, the attorney privilege applies, even if there were also other purposes for the investigation and even if the investigation was mandated by regulation rather than simply an exercise of company discretion."[39] In other words, the correct test under the D.C. Circuit, Clark Hill argues, is not whether a communication would have been made but for the fact that legal advice was sought, but rather whether obtaining or providing legal advice was "one of the significant purposes" of the communications.

The court does not address the "significant purpose" test head-on, instead noting that the communication must be made for "the purpose" of obtaining or providing legal advice, and then walking through a brief factual analysis of the forensic consultant report that concludes with the finding that Clark Hill's "true objective" was not to obtain legal advice from its lawyers but instead to obtain cybersecurity expertise from the forensic consultant.[40] The court instead focuses on whether the *Kovel* doctrine should apply to such a forensic report, noting that Clark Hill "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."[41] The court distinguishes *Target* by noting that Target had a two-track approach (which the court does not find here), there is no indication that the Target report was shared as widely for non-legal purposes, and the *Target* court noted that the relevant report was not focused on remediation of the breach.[42]

---

[35] Memorandum in Support of Plaintiff's Motion for an Order Compelling Discovery, at 12.
[36] *Id.* at 13.
[37] Response to Motion to Compel, at 18.
[38] *Id.* at 18 (citing *Kellogg*, 756 F.3d at 759).
[39] *Id.* at 19 (citing *Kellogg*, 756 F.3d at 758-59 (emphasis added)).
[40] Mem. Op. at 15-16.
[41] *Id.* at 17.
[42] *Id.*

Part Four: The Opinion Highlights Several Lessons for Companies Seeking to Conduct a Privileged Investigation.

There are several steps that may be useful for maximizing the likelihood that a court will find that investigation-related communications and a written forensic report are protected as attorney-client or work product privileged communications.

A. Limiting the Scope, Purpose, and Audience of Privileged Reports.

Companies should carefully consider the recipients of any report produced by a third-party firm under privilege, limiting the number of both internal and external recipients as much as possible and as appropriate, especially the full report. Companies should also consider the scope and purpose of any written reports prepared by external parties, recognizing that the broader the scope of the report (e.g., whether the report includes broader security recommendations and improvement), the more difficult it may be to persuasively demonstrate that the purpose of the report was to obtain legal advice regarding the incident.

B. Demonstrating a Two-Track Approach.

If a company is using a two-track approach, companies should consider how to distinguish any ordinary-course incident investigation from a privileged investigation.

For an "ordinary course of business" investigation, a company may consider generating a non-privileged summary of attacker activity to illustrate that the internal investigation resulted in specific investigative findings and conclusions designed to inform the company of what happened and how to remediate and contain the identified activity. Conversely, companies should carefully consider the role of reports generated by a third party engaged by counsel. For example, does it supplement a company's understanding of its legal obligations following a cyber incident, or does it serve as the basis for the company's entire understanding of an incident? It may be easier to defend privilege if the purpose is the former.

C. Defending Attorney-Client Privilege and the Work Product Doctrine.

It is worth noting that just as the court did not spend as much time addressing attorney-client privilege in contrast to the work product doctrine, Clark Hill also did not spend as much time discussing attorney-client privilege in its brief on this issue. In particular, Clark Hill did not focus on the *Kovel* doctrine and how broadly it should be applied. It is possible that this played a role in the court's decision to apply the doctrine narrowly. Regardless, this case serves as a reminder that legal teams should carefully review (and internal protocols must be consistent regarding) the retention, management, and documentation of third parties engaged to assist in incident response in order to maximize the strength of a company's claim for attorney-client privilege and protection under the work product doctrine.

Recommended Practices for Protecting Work Product

The following are other recommended practices to consider for protecting work product during the security incident investigation process based on the *Capital One* decision and other recent case law development.

(1) If you have a prior relationship with the forensic firm investigating the security incident, ensure the scope of services for the forensic firm statement of work (SOW) with counsel differs from previous SOWs and retainers.
(2) Revisit the language of existing agreements with cybersecurity vendors to include reference to privileged work and include a template privileged/work product SOW.
(3) When possible, pay the forensic firm investigating the security incident with funds from your legal budget, not your information security budget.
(4) Consider having multiple vendors or no continuous business relationship with the forensic firm.
(5) Consider multiple iterations of forensic work product so that only the general counsel's office receives the full report and limit dissemination of the full report.