July 17, 2020

The Honorable John M. Facciola (Ret.) <facciolj@georgetown.edu>

Re: *In re: Marriott,* MDL 2879 (D. Md.), CrowdStrike Investigation

Dear Special Master Facciola:

In response to certain suspicious anomalies regarding the Starwood guest reservation database, Marriott retained a forensic investigator with whom it already had an ongoing business relationship (a cybersecurity firm called CrowdStrike Services, Inc. ("CS")) to take the lead investigating and remediating its data breach. CS's mandate was broad: Marriott directed it to provide an initial "triage" of the breach, investigate, develop a remediation plan and assist Marriott in carrying it out, and make recommendations for long-term security improvements.

Despite the fact CS was re-retained for the business-critical purposes of investigating and remediating a large-scale breach affecting millions of Marriott's customers, Marriott asserts that CS's work is privileged and work product. Specifically, Marriott argues that its outside counsel, BakerHostetler ("BH"), retained CS *on Marriott's behalf* solely to assist the firm in providing legal advice. But, BH has attempted this maneuver before and courts have rejected BH's attempts to manufacture privilege claims for its clients by mischaracterizing a factual breach investigation as "work product." *See generally In re Dominion Dental Servs. USA, Inc. Data Breach Litig*., 429 F. Supp. 3d 190 (E.D. Va. 2019); *In re Premera Blue Cross Customer Data Sec. Breach Litig*., 296 F. Supp. 3d 1230 (D. Or. 2017) ("*Premera I*"). Having failed to prevent the disclosure of forensic reports in these past cases, BH conjured up a new strategy here: BH evidently instructed CS to perform its usual functions—including conducting a forensic analysis to determine the size and scope of the breach—but to forego preparing a formal "report." Instead, CS documented its findings internally and then relayed its conclusions to select Marriott personnel (and third parties) through a series of regular telephone calls, videoconferences, and weekly status reports. These communications were used to disseminate critical business information with lawyers present to ostensibly support an argument that such communications are privileged.

Unfortunately for BH and Marriott, BH's scheme ignores that it is the *substance* of the communications that dictate privilege—not how or to whom they are communicated. Accordingly, Plaintiffs respectfully request that the Court follow the rationale of every recent court to consider this issue (including two in this Circuit) and order Marriott to produce: (1) all agreements and statements of work entered into by and between CS and Marriott/Starwood (or its counsel) pre- and post-dating the breach; (2) all investigations, reports, assessments, decisions, findings, conclusions, and recommendations prepared or documented by CS pursuant to its statement of work with Marriott following discovery of the breach regardless of form; (3) all communications between Marriott and CS regarding CS's investigations, reports, assessments, decisions, findings, conclusions, and recommendations, including meeting agendas, status reports, PowerPoint presentations, and related materials; (4) all communications between Marriott employees regarding CS's post-breach investigations, reports, assessments, decisions, findings, conclusions, and recommendations; and (5) all memoranda, notes, and communications prepared by Marriott's employees reflecting conversations between CS and Marriott. The Parties have met and conferred on numerous occasions on this subject and are at an impasse.

LEGAL STANDARDS

The legal standards governing work product and privilege in this Circuit were detailed extensively in two recent and analogous cases and are referenced herein. *See generally In re Capital One Consumer Data Sec. Breach Litig.*, 2020 WL 2731238, at *3 (E.D. Va. May 26, 2020), *report & recommendation adopted*, No. 1:19-md-02915, Dkt. 641 (E.D. Va. June 25, 2020); *Dominion Dental*, 429 F. Supp. 3d at 194. In short, (1) the party asserting protection bears the burden of proving it; (2) materials prepared in the ordinary course of business or that would have been created in essentially similar form irrespective of litigation are not work product; (2) underlying facts cannot be shielded from disclosure; and (3) even fact work product can be discoverable if a party shows substantial need for the materials to prepare its case and that they cannot, without undue hardship, obtain their substantial equivalent by other means. *Id.*

I. CS'S INVESTIGATION IS NOT WORK PRODUCT.

When Marriott retained CS to investigate the breach, Marriott did not know the cause or extent of the breach. Determining how the breach occurred and identifying efforts necessary to remediate the security failures that caused it are not "legal investigations." As a matter of common sense, CS performed a factual investigation that was critical to Marriott's entire business operations and would have been conducted in the absence of litigation or Marriott's retention of counsel. CS's work does not qualify as work product because the "driving force" behind CS's work was entirely business-related, not litigation.

This is especially true where, as here, a party had a pre-existing relationship with the third-party investigator and the work likely would have been performed regardless of whether it was directed by counsel. *See, e.g., Capital One*, 2020 WL 2731238, at *4 ("Capital One had a long-standing relationship with [forensic investigator] and had a pre-existing SOW with [investigator] to perform essentially the same services that were performed in preparing the subject report"); *Dominion Dental*, 429 F. Supp. 3d at 195 (investigator had existing scope of work pre-dating discovery of the breach); *Premera I*, 296 F. Supp. 3d at 1245 (same). Here, CS previously performed forensic work for Marriott and the parties agreed on a multi-year contract for such services prior to discovery of the breach.[1] **Ex. A**, MI_MDL_01257247 (correspondence from CS to Marriott in March 2018: "Attached are two separate reports [from CS] one ... is the custom analysis of what we saw in your environment and the other ... is how we have seen this adversary operating with this tool on a broader global scale."). Indeed, Marriott had already engaged CS to provide its Falcon tool in early September 2018 to improve threat detection and response on the Marriott network (**Ex. B**, MI_MDL_00946533.pptx, produced in .pdf format for this letter) and this tool actually uncovered the breach at issue. **Ex. C**, MI_MDL_00467547. Marriott simply asked CS to continue its ongoing work, but added counsel in feeble attempt to avoid discovery.

Additionally, the new Statement of Work Marriott executed with CS on September 12, 2018, after discovery of the breach shows that CS's work was *business* driven. In the SOW, CS agreed to "assist Customer"—defined as Marriott, *not legal counsel*—"with responding to a potential computer security incident." **Ex. D**, MI_MDL_00955464. The SOW divided CS's work into three phases. *Id.* at 465. In "Phase 1: Incident Triage," CS committed to analyzing data *provided by Marriott*; discussing "business concerns related to the incident"; discussing the

[1] Marriott also had relationships with other, third-party service providers before the breach, such as IBM. Plaintiffs' counsel has served subpoenas to third parties for relevant documents, and understands that Marriott's counsel intends to claim work product protection over certain of those documents, as well—an issue which will be brought to the Special Master's attention when ripe.

incident *with Marriott's staff*; and producing a "summary report with recommended next steps and effort estimates." In "Phase 2: Investigation and Remediation," CS was tasked with determining compromised systems, analyzing Marriott's network; setting up CS Falcon products on Marriott hardware devices; planning a "remediation event to deny the attacker further access" to Marriott's systems; and assisting Marriott "in conducting the remediation event." Finally, in "Phase 3: Strategic recommendations," CS agreed to "[p]rovide recommendations for long-term continuous security posture improvement." *Id*. Thus, the SOW makes clear that CS's responsibilities were related to *Marriott's* company-wide investigation into the breach, remediation, and then ultimately to provide recommendations on long-term changes to improve Marriott's security. Marriott cannot credibly claim, least of all meet its burden to show, that it would not have conducted the investigation but for the anticipated threat of litigation as it needed to uncover and remediate the breach to protect its customers. Other courts have recognized that a forensics firm investigating a data breach in similar circumstances does not warrant work product protection. *See, e.g.*, *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 329 F.R.D. 656, 666 (D. Or. 2019) ("*Premera II*") ("[D]iscovering how the breach occurred was a necessary business function regardless of litigation or regulatory inquiries. Premera needed to conduct an investigation as a business in order to figure out the problem that allowed the breach to occur so that Premera could solve that problem and ensure such a breach could not happen again.").

Marriott will argue that everything within the SOW is privileged because BH inserted itself as a party to the SOW and because the SOW states that BH "is engaging [CS] on behalf of Customer to perform the Services . . . ." **Ex. D**. This, however, is a sham designation that the Court should disregard for several reasons. As discussed, the "Services" that CS actually provided (*e.g.*, leading Marriott's factual investigation and remediation of the breach) far exceed assistance with the provision of legal advice. The Court should be even more suspicious of Marriott's assertion because it is company policy to claim privilege over any work done by third-party forensics firm, regardless of whether that work actually qualifies as privileged. Marriott's Incident Response Plan contains a section dedicated to retaining outside forensics firms that states that "[a]ll third-party forensics vendors will be retained through Group Legal to maximize the extent to which the attorney-client privilege and work product doctrines apply to the investigation." **Ex. E**, MI_MDL_00003197 at 3219. The Plan also notes that, "generally, the attorney-client privilege only applies to documents and communications seeking or providing legal advice, and not to every document or communication labeled as 'Attorney-Client Privileged' or which includes Group Legal or outside counsel in the distribution." *Id.* at -3218. Even though "blanket assertions" of privilege are disfavored, that is exactly what Marriott has made here and the Court should reject it.

The Court should also reject the argument that CS's investigation is protected because its findings were communicated to Marriott verbally (or through other means) rather than as a written report. First, Marriott's documents reflect that regular meetings were set with Marriott's *business* personnel for the purpose of discussing CS's findings, contradicting any argument that CS's work was performed for the purpose of providing legal advice. *See, e.g.*, **Ex. F**; MI_MDL_02465828 (calendar invitation to numerous Marriott employees regarding update on "Project Phoenix"—One of CS's code words for the breach). Other documents suggest that CS was also providing Marriott with regular written documents reflecting its findings—with Marriott requesting on at least one occasion a "less technical executive summary" for its executives. *See, e.g.*, **Ex. G**, MI_MDL_01686512 ("Please find this week's report from CS"). Marriott also established an internal repository for CS-related materials to assist its own investigation. **Ex. H**,

MI_MDL_01446081 ("[A]nother SharePoint site . . . has been established for Project Phoenix . . . it houses many of the materials and documents you may find helpful."). Documents prepared by CS for these meetings or notes taken by Marriott personnel during these meetings were necessary to perform *business* remediation and investigative functions and cannot possibly be considered attorney work product. Second, based upon BH's representations that there is no CS report, it is apparent BH instructed CS to withhold a final report in order to sidestep its unsuccessful track record of preventing the disclosure of third-party reports in other data breach cases. *See* discussion *supra*. But the rationale underlying those opinions applies the same regardless of whether CS prepared a final written report. Finally, any work product protections that might have existed were waived as these materials were shared with third parties. **Ex. I**, MI_MDL01461473, -491 (noting the sharing of all CS materials with Ernst & Young), **Ex. F**, MI_MDL_02465828 (sharing Project Phoenix update with employees of Kroll, a third pary investigator).

In *Dominion Dental*, Judge Nachmanoff of the U.S. District Court for the Eastern District of Virginia ordered the defendants to produce a forensics investigation report produced by a competitor of CS called FireEye Mandiant. 429 F. Supp. 3d at 191. The Court noted that Dominion's attempt to use its outside counsel BH as a go-between was "designed to help shield material from disclosure" rather than reflect the actual relationship between the defendant, outside counsel, and Mandiant. *Id*. at 194. Despite an affidavit from Dominion that the Mandiant report would not have been prepared in a substantially similar form and may not have been necessary at all without the threat of litigation, the Court found that conclusion was contradicted by the report itself which contained information that was "entirely factual, relates directly to the business interests of the defendants, and does not appear to include legal analysis or attorney work product." *Id.* at 194, n.4. The SOW at issue here strongly suggests that any of CS's findings would be the same.

In *Premera*, Judge Michael H. Simon in the District of Oregon ordered Premera Blue Cross to produce the Mandiant report and related non-privileged or work-product communications. In that case, Judge Simon concluded that Mandiant's work was *not* performed as an investigator working on behalf of BH as required to invoke protections, but was performing a necessary business function that would have occurred in the absence of litigation. *Premera II*, 329 F.R.D. at 666.

And, more recently, the Eastern District of Virginia relied on *Dominion Dental* and *Premera* to conclude that a third-party report prepared for Capital One was not protected where Capital One could not show that "Mandiant's scope of work under the Letter Agreement with outside counsel was any different than the scope of work for incident response services set forth in the existing SOW and that it would not have been performed without the prospect of litigation." *Capital One*, 2020 WL 2731238, at *6.

As in these cases, and regardless of whether CS shared its findings with Marriott in a formal report or as part of regular meetings and status reports, Marriott cannot credibly claim that it would not have conducted the investigation but for the anticipated threat of litigation. Because the "driving force" behind CS's work was for business purposes, the Court should conclude that the CS investigation is not protected as work product and order it produced.

II. CS'S WORK IS NOT PROTECTED BY PRIVILEGE.

The CS investigation is not protected by the attorney-client privilege. CS is a data security expert, not a legal expert. Its investigation could not have been performed using any legal expertise or itself provided legal advice to Marriott. *Cf. In re Allen*, 106 F.3d 582, 602-03 (4th Cir. 1997)

(finding attorney hired to conduct factual investigation was "retained to conduct an investigation using her legal expertise" but recognizing that no privilege attaches when investigation is performed in a capacity other than as a lawyer). In order for the attorney-client privilege to attach, Marriott bears the burden to prove that CS's work was performed with the intention of securing legal advice. *Greenberg v. State of Maryland*, 26 A.3d 396, 959 (Ct. App. Md. 2011). Marriott cannot do so. Marriott's Board Minutes, in updates given by non-lawyers, state that CS's role is "taking the lead on the forensic analysis of the" breach. **Ex. J**, MI_MDL_01128852 at 853. Although Marriott's counsel may have provided legal services utilizing CS's work, CS's investigation would have been done regardless given that millions of guest records were breached.

III. PLAINTIFFS HAVE SUBSTANTIAL NEED FOR THE CS MATERIALS.

Assuming, *arguendo*, the Court concludes that CS's investigation is work product, it should nevertheless compel Marriott to produce it under the exception in Rule 26(b)(3)(A). Plaintiffs have a substantial need for the investigative materials and it will be impossible or unduly difficult for Plaintiffs to obtain the same information through other means. CS's investigation details Marriott's data security failures that led to or contributed to both the data breach itself and Marriott's failure to discover the data breach for four years. These are crucial liability materials that will enable Plaintiffs to prosecute their case more efficiently. Indeed, production of the investigation materials will necessarily streamline the discovery process, which will benefit Marriott as well. As it stands, Marriott has provided minimal information about the cause of the data breach, despite the fact that Marriott already knows this information. In addition, attempting to obtain the same information contained in the CS's materials will impose undue hardship on Plaintiffs. *See* **Ex. K**, Declaration of Mary Frantz ("Frantz Decl."). Plaintiffs will have to obtain and search through thousands of documents and communications—many of which are archived, some of which may be destroyed, and most of which have no relevance to the breach at all—to piece together and identify these deficiencies that CS already uncovered. *Id*., ¶¶ 36-37. While Marriott may point to the fact that it preserved its servers in the same condition as when CS conducted its investigation, this is insufficient because the contemporaneous analysis done by CS provides the only reliable snapshot of the evidence uncovered during the investigation. *Id.*, ¶¶ 36-37. Moreover, unlike CS, Plaintiffs will not have the ability to question Marriott data security and infrastructure employees at will. They will be confined to single depositions, the preparation for which will require Plaintiffs to have already reached their conclusions regarding the cause of the breach and Marriott's failure to discover it. This would take years of painstaking discovery at considerable time, expense, and effort of the parties and Court—in direct contravention to the directives of Fed. R. Civ. P. 1. Moreover, Plaintiffs have brought claims for injunctive relief and are entitled to know the entire universe of remediation recommendations presented to Marriott. If CS made deficiency findings that Marriott has not corrected or remediation recommendations that it has not implemented, this information can only be discovered—and more importantly confirmed—by actually reviewing CS's conclusions and work product, in whatever form they exist.

For all the reasons set forth above, Plaintiffs request that the Court issue an order compelling Defendants to produce CS materials as outlined herein.

Respectfully,

/s/ Amy E. Keller */s/ Andrew N. Friedman* *Co-Lead Counsel, Consumer Track*[2] */s/ James J. Pizzirusso*

[2] Counsel in the Financial Institution and Government Tracks support the relief sought in this letter.