August 14, 2020

To: The Honorable John M. Facciola, *via email* at facciolj@georgetown.edu

Re: *In re: Marriott*, MDL 2879 (D. Md.), Response to Plaintiffs' July 17, 2020 letter

Months ago, consistent with your guidance, Marriott proposed a categorical privilege logging protocol (Ex. A). Plaintiffs only recently responded—not with a substantive counterproposal but simply stating they do not want categorical logging. Before concluding these negotiations,[1] much less reviewing the resulting log, plaintiffs moved to compel production of broad categories of documents related to CrowdStrike's forensic work. Plaintiffs' five categories, save the first one, are overlapping and vague. To focus the issues, Marriott provides the following more precise categories and Marriott's corresponding position. Marriott also will not object to a deposition of CrowdStrike regarding facts. Indeed, the U.S. regulators interviewed CrowdStrike under these parameters, and had no issue not delving into work-product or attorney/client privileged territory.

No.	Category of Documents	Marriott's Position
1	CrowdStrike Statements of Work.	Produce relevant documents (i.e., those regarding the Starwood network).
2	Marriott communications regarding the mechanics of installing Falcon and FFC.	Produce relevant documents (redacted if a privileged category is also included).
3	Device images, logs, and FFC output files collected and reviewed by CrowdStrike.	Produce relevant documents.
4	CrowdStrike's review, explanation, and interpretation of the incident (i.e., to or from CrowdStrike).	Attorney/client privileged and/or work product. Examples are being submitted *in camera* as Exhibits D through G.
5	Internal Marriott documents reflecting gathering of facts and data to support Category 4.	Attorney/client privileged and/or work product. Examples are being submitted *in camera* as Exhibits H through I.
6	Internal Marriott documents reflecting Category 4.	Attorney/client privileged and/or work product. Examples are being submitted *in camera* as Exhibits J through N.
7	Internal Marriott documents reflecting legal advice and communications regarding the security incident.	Attorney/client privileged and/or work product. Exhibits J through N also include Category 7.

Background. On September 7, 2018, Accenture was alerted to a suspicious query of the Starwood Guest Reservation Database, which it managed for Marriott. Marriott and Accenture investigated and learned that the employee whose credentials were used did not perform the query. (Declaration of Craig Hoffman ¶¶ 8-9, Ex. B.)

This type of unauthorized activity implicates a host of legal issues under myriad laws. For example, Maryland law defines a "breach of the security of a system" as "the unauthorized

[1] Marriott will provide a document-by-document log should the Court deem it useful to resolving this dispute.

acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a business." MD Comm. Code § 14-3504(a)(1). If this occurs, an investigation must be completed to determine whether information may be misused and, if so, whether there is a legal duty to notify customers and regulators. *Id.* § 14-305(b)(1) & (h). Marriott operates across the country and around the world, and other states and countries also have notification requirements that operate in similar, and sometimes dissimilar, ways. (Hoffman Dec. ¶ 4.) Many statutes also include data security standards. *See* MD Comm. Code § 14-3503(a). Moreover, there are also contractual arrangements that incorporate data security standards and impose contractual obligations to notify card brands of security incidents potentially affecting payment card data under some circumstances. (Hoffman Dec. ¶ 5.)

Promptly after learning that these laws and contractual obligations might be at issue, Marriott engaged BakerHostetler to advise Marriott regarding Marriott's legal obligations. (Hoffman Dec. ¶¶ 10-11; Declaration of John Warren ¶¶ 12-14, Ex. C.) And because litigation is common when a business suffers a cyberattack, Marriott anticipated litigation was imminent. (Warren Dec. ¶¶ 15-19; Hoffman Dec. ¶ 6.) Lawyers on their own do not have the specialized tools and knowledge to gain an understanding of their client's technical information relevant to a data security incident. (Hoffman Dec. ¶ 12.) A lawyer must rely on forensics experts to translate a client's technical information so that the lawyer can provide legal advice. (*Id.* ¶¶ 13-17.) BakerHostetler engaged CrowdStrike to perform this role. (*Id.* ¶ 18.)[2]

BakerHostetler retained CrowdStrike so it could provide legal advice and in anticipation of litigation. (*Id.* ¶¶ 18-32; Warren Dec. ¶¶ 20-24.) CrowdStrike worked at the direction of BakerHostetler to help counsel understand the technical information relevant to the incident. (*Id.*) CrowdStrike's work included installing specialized tools across Marriott's network and then analyzing and interpreting the collected information. (*Id.*) This analysis was necessary for counsel to provide Marriott with legal advice about issues arising from the security incident. (*Id.*)

Law and Argument. *Attorney/client privilege*. For attorney/client privilege to attach to a communication, it must be "made between privileged persons," "in confidence," and "for the purpose of seeking, obtaining, or providing legal assistance to the client." *Richardson v. Sexual Assault/Spouse Abuse Res. Ctr., Inc.*, 764 F. Supp. 2d 736, 742 (D. Md. 2011). Attorney/client privilege exists independent of any anticipation of litigation.

As described in the attached declarations, Marriott sought advice from BakerHostetler regarding legal issues associated with a potential data security breach, including whether and when notification was required and how Marriott could comply with its obligations under various data security laws and standards. That engagement generated communications reflecting counsel's factual investigation and the advice and consultation that flowed from the investigation regarding Marriott's legal obligations under the laws and contracts described above. (*See, e.g.*, Exs. J – K.)

These documents are privileged under well-established law. A lawyer's discussion with his or her client regarding the underlying facts and associated legal obligations is at the core of the attorney/client privilege. *See In re Search Warrant Issued June 13, 2019*, 942 F.3d 159, 173 (4th

[2] Mr. Hoffman is available to discuss the necessity of forensic analysis and the resulting legal advice flowing from that analysis should the Court deem it useful to resolving this dispute.

Cir. 2019) ("the attorney-client privilege exists because sound legal advice or advocacy serves public ends and such advice or advocacy depends upon the lawyer's being fully informed by the client") (quotation omitted). And attorney factual investigations "fall comfortably within the protection of the attorney-client privilege." *Sandra T.E. v. S. Berwyn Sch. Dist. 100*, 600 F.3d 612, 619 (7th Cir. 2010) (describing *Upjohn Co. v. United States*, 449 U.S. 383 (1981)).

Importantly, this privilege also extends to CrowdStrike's communications with BakerHostetler and Marriott (Category 4) because privileged persons include "retained professionals who assist the attorney to better understand the facts in providing competent legal advice to the attorney's client." *Richardson*, 764 F. Supp. 2d at 742 (citing *United States v. Kovel*, 296 F.2d 918, 921 (2d. Cir. 1961)). The Second Circuit's oft-cited decision in *Kovel*, where the presence of an accountant did not destroy the privilege, analogized the situation to "the client speaking a foreign language": "Accounting concepts are a foreign language to some lawyers in almost all cases, and to almost all lawyers in some cases." 296 F.2d at 922. Thus, "the presence of an accountant, whether hired by the lawyer or by the client, while the client is relaying a complicated tax story to the lawyer, ought not destroy the privilege, any more than would that of the linguist in the second or third variations of [a] foreign language[.]" *Id.*

Similarly, BakerHostetler engaged CrowdStrike to effectively translate the technical information residing on Marriott's systems, which was essential for BakerHostetler to advise Marriott about the legal implications of the incident and prepare Marriott for impending litigation. (Hoffman Dec. ¶¶ 12-17; Warren Dec. ¶ 20.) The documents submitted *in camera* reflect this relationship and the necessity of the engagement. (*See* Exs. D – G.)

This privilege exists even if employees are communicating outside the presence of counsel regarding efforts to gather facts (*see, e.g.*, Exs. H, I, and N; *see also* Hoffman Dec. ¶ 26), or if Marriott employees are discussing or relaying CrowdStrike's findings or counsel's advice to others in the organization (*see, e.g.*, Ex. L). "[W]here the client is a corporation, documents subject to the privilege may be transmitted between non-attorneys to relay information requested by attorneys." *Bluestem Brands, Inc. v. Merkle, Inc.*, 2014 WL 12736150, at *2 (D. Md. Nov. 19, 2014) (quoting *Santrade, Ltd. v. Gen. Elec. Co.*, 150 F.R.D. 539, 545 (E.D.N.C. 1993)). Similarly, "documents subject to the privilege may be transmitted between non-attorneys (especially individuals involved in corporate decision-making) so that the corporation may be properly informed of legal advice and act appropriately." *Id.*; *see also Sky Angel U.S., LLC v. Discovery Commc'ns, LLC*, 28 F. Supp. 3d 465, 486 (D. Md. 2014) ("Communications among non-attorneys in a corporation may be privileged if made at the direction of counsel[ ] to gather information to aid counsel in providing legal services[.]").

Plaintiffs argue that board minutes state that CrowdStrike took "the lead on the forensic analysis of the cyber incident," so, according to plaintiffs, CrowdStrike's work was not "performed with the intention of securing legal advice." (Pl. Ltr. 5 & Ex. J.) But the same sentence says that counsel engaged CrowdStrike, and, in fact, BakerHostetler directed the forensic analysis. (Hoffman Dec. ¶¶ 18-25.) In any event and in plaintiffs' own words, "it is the *substance* of the communications that dictate privilege." (Pl. Ltr. 1 (emphasis in original).) The declarations and communications submitted *in camera* show that CrowdStrike was a "retained professional[] who assist[ed Marriott's attorneys] to better understand the facts in providing competent legal advice to [Marriott]." *Richardson*, 764 F. Supp. 2d at 742.

Courts apply this rationale to the communications of forensic consultants in data security cases. *See Genesco, Inc. v. Visa U.S.A., Inc.*, 302 F.R.D. 168, 190 (M.D. Tenn. 2014) (under *Kovel*, "privilege extends to the [forensics] firm that assisted counsel in [counsel's data security] investigation"); *In re Target Corp. Customer Data Sec. Breach Litig.*, 2015 WL 6777384, at *3 (D. Minn. Oct. 23, 2015) (communications with consultant informing "counsel about the breach so that Target's attorneys could provide the company with legal advice" were privileged).

The cases on which plaintiffs rely addressed work product (and are addressed below); they did not turn on the application of the attorney/client privilege. *See In re Dominion Dental Servs. USA, Inc. Data Breach Litig.*, 429 F. Supp. 3d 190 (E.D. Va. 2019), *In re Premera Blue Cross Cust. Data Sec. Breach Litig.*, 296 F. Supp. 3d 1230, 1245-46 (D. Or. 2017), and *In re Capital One Cons. Data Sec. Breach Litig.*, 2020 WL 2731238 (E.D. Va. May 26, 2020).

Work product. "Rule 26(b)(3)(A) protects from disclosure documents and other tangible items 'prepared in anticipation of litigation or for trial by or for another party or its representative,' [including] a party's consultant." *Goldstein v. F.D.I.C.*, 494 B.R. 82, 90 (D.D.C. 2013). A document is protected "when the party faces an actual claim or a potential claim following an actual event or series of events that reasonably could result in litigation **and** the work product would not have been prepared in substantially similar form but for the prospect of that litigation." *Capital One*, 2020 WL 2731238, at *3 (emphasis in original).

When Marriott learned an unauthorized person or persons accessed its network, it anticipated litigation and thus immediately hired a firm experienced in investigating and litigating data security incidents. (Hoffman Dec. ¶¶ 10-12; Warren Dec. ¶¶ 17-18.) The anticipation was well founded: nearly 100 cases were filed.

Plaintiffs say CrowdStrike's work nonetheless is not "work product because the 'driving force' behind CS's work was entirely business-related, not litigation." (Pl. Ltr. 1.) Not so. Documents reflecting CrowdStrike's work to analyze and explain Marriott's technical information and communications with Marriott and counsel about that work, "would not have been prepared in substantially similar form but for the prospect of that litigation." *Capital One*, 2020 WL 2731238, at *3. Marriott was working with counsel, assisted by CrowdStrike, to prepare for litigation with regulators and private plaintiffs. (Hoffman Dec. ¶¶ 19-32; Warren Dec. ¶ 24.)

As the Sedona Conference recently recognized, in the cybersecurity context "counsel often will work with technical experts within the legal organization or hire technical experts to assist in creating a legally prioritized remediation report." Sedona Conference, *Privilege and Protection in the Cybersecurity Context*, 21 SEDONA CONF. J. 1 (forth. 2020), at 30-31. These "[a]ssessments prioritized by reference to the legal standards and environment in which the company operates, and conducted under the supervision of counsel, contain legal decisions about what is reasonable under the law for the particular organization." *Id.*

Plaintiffs rely on decisions in *Capital One*, *Dominion*, and *Premera*. But these cases, apart from being distinguishable (as explained below), take too narrow a view of work product in the cybersecurity context. That narrow view has an "undesirable chilling effect on conducting frank and pointed analyses" of cybersecurity. *Id.* at 78.

These cases also concluded that because an investigation was later used for a business purpose, it must have been conducted for that purpose. *See Dominion*, 429 F. Supp. 3d at 194; *Capital One*, 2020 WL 2731238, at *4. But "a document can contain protected work-product material even though it serves multiple purposes, so long as the protected material was prepared because of the prospect of litigation." *United States v. Deloitte LLP*, 610 F.3d 129, 138 (D.C. Cir. 2010). Under the "because of" test, applied in the Fourth Circuit, "material generated in anticipation of litigation may also be used for ordinary business purposes without losing its protected status." *Id.*; *see also id.* at 136 (aligning with Fourth Circuit).

This case also differs materially from *Dominion*, *Capital One*, and *Premera*. Unlike in those cases, two separate forensics firms reviewed the incident here. Verizon prepared a global report about the incident for Marriott, which plaintiffs already have. CrowdStrike's separate, confidential investigation is work product. *See Target*, 2015 WL 6777384, at *3 (work product applied to confidential investigation); *Parsons v. Kimpton*, N.D. Cal. Case No. 3:16-cv-05387, ¶ 2 (February 20, 2018), attached as Ex. Q (same).

Plaintiffs accuse BakerHostetler of instructing CrowdStrike not to prepare a comprehensive report for some nefarious reason. But plaintiffs never explain why CrowdStrike would have necessarily prepared such a report. In fact, the lack of a comprehensive report is consistent with CrowdStrike's role: CrowdStrike advised counsel so that counsel could provide legal advice and prepare for litigation—work that does not require a comprehensive report. (Hoffman Dec. ¶ 30.)

Plaintiffs briefly mention waiver of work product because "materials" were shared with Marriott's auditor and Kroll. (Pl. Ltr. 4.) Plaintiffs are wrong. Project Phoenix is not a CrowdStrike codename; it is the name for the cyberattack. (Warren Dec. ¶ 27.) Moreover, work product is only waived if disclosed to an adversary. *In re Doe*, 662 F.2d 1073, 1081 (4th Cir. 1981). Neither Kroll nor Marriott's auditors were an adversary. *Deloitte*, 610 F.3d at 139-143.

Nor do plaintiffs have a "substantial need" for the materials. Only fact, not opinion, work product may be discovered based on a substantial need. *Goldstein*, 494 B.R. at 90. But much of the information contained in the documents are the opinions and mental impressions of CrowdStrike and Marriott's counsel. *See Duplan Corp. v. Deering Milliken, Inc.*, 540 F.2d 1215, 1219 (4th Cir. 1976) ("opinion work product immunity now applies equally to lawyers and non-lawyers alike") (quotation omitted). (*See, e.g.*, Exs. M and O.)

Plaintiffs will have access to all of the underlying facts from numerous sources, including the PFI Report and the underlying servers themselves. (Warren Dec. ¶¶ 28-30.) Having to analyze the facts rather than intrude on the work of BakerHostetler does not create a substantial need. *See, e.g., Fed. Trade Comm'n v. Staples, Inc.*, 2016 WL 259642, at *4 (D.D.C. Jan. 21, 2016) (plaintiffs may "not simply freeload on opposing counsel") (quotation omitted).

Conclusion. The Court should deny plaintiffs' motion to compel.

/s/ *Gilbert S. Keteltas*

EXHIBIT A

EMAIL CORRESPONDENCE

From: Busen, Carey
Sent: Sunday, May 31, 2020 9:32 AM
To: Ariana Tadler
Cc: Keteltas, Gilbert S.
Subject: Priv log protocol
Attachments: 2020 05 31 DRAFT Marriott Proposed Privilege Log Order.docx

Ariana,

I hope you are well. Attached please find a draft privilege logging protocol for your side's consideration. I trust that you will circulate to the proper people on all three tracks, but let me know if that is an incorrect assumption.

Thank you and have a pleasant Sunday.
Carey

Carey S. Busen
Partner

BakerHostetler

Washington Square
1050 Connecticut Ave, N.W. | Suite 1100
Washington, DC 20036-5403
T +1.202.861.1568

cbusen@bakerlaw.com
bakerlaw.com

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
Southern Division

IN RE: MARRIOTT INTERNATIONAL CUSTOMER DATA SECURITY BREACH LITIGATION	*	MDL No.: 19-md-2879
	*	JUDGE GRIMM
THIS DOCUMENT RELATES TO THE CONSUMER, FINANCIAL INSTITUTION, AND GOVERNMENT TRACKS	*	

* * * * * * * * * * * * * * *

STIPULATED PROTOCOL AND [PROPOSED] ORDER FOR THE LOGGING OF PRIVILEGED ELECTRONICALLY STORED INFORMATION

WHEREAS the review of documents and electronically stored information ("ESI") to isolate, withhold and describe privileged materials can impose substantial costs on the producing party;

WHEREAS the burden and complexity of privilege review and logging of privileged materials are magnified in the case of discovery of ESI given the volume of data and nature of electronic communications;

WHEREAS a traditional document-by-document privilege log may not be an effective or efficient means to assess the accuracy of privilege claims in ESI-intensive matters; and

WHEREAS the parties seek to reduce the burdens and delay, and enhance the accuracy of, privilege review while minimizing the risk of privilege waiver,

WHEREAS the parties reserve the right to amend this Protocol in the event any Complaints in the Actions are amended or supplemented;

The Parties stipulate and agree to this proposed order establishing a protocol for the review, treatment and logging of privileged documents and ESI. The Court, having reviewed the

Parties' stipulated order, adopts the parties' stipulation to streamline the production of a log of privileged ESI and to promote a "just, speedy, and inexpensive determination" of this action, as required by Federal Rule of Civil Procedure 1, hereby ORDERS:

A. Definitions

1. "Actions" shall mean the cases coordinated or consolidated for pre-trial proceedings in this multidistrict litigation captioned In re Marriott International Customer Data Security Breach Litigation, MDL No. 19-md-2879.

2. "Agent(s)" shall mean certain third-party vendors engaged by Counsel for the purpose of providing legal advice.

3. "Counsel" shall mean attorneys who are employees of a Party or attorneys who are not employees of a Party, but who are retained to represent or advise a Party.

4. "Disclosing Party" shall mean a Party that discloses information in a privilege log about information withheld from discovery on privilege grounds.

5. "Incident" shall mean the Starwood database security incident that is the subject of the Actions.

6. "Party" shall mean any party to the Actions, including all of its officers, directors, and employees.

7. "Privileged Documents" shall mean information withheld from productions based on the attorney-client privilege, work-product doctrine, or any other applicable privilege or protection.

8. "Receiving Party" shall mean a party that receives a privilege log from a Disclosing Party.

B. Scope

The procedures outlined herein govern the format of a categorical privilege log for documents withheld, in whole or in part, from production based on attorney-client privilege, work-product doctrine, or any other applicable privilege or protection. Except as expressly stated, nothing in this order affects the Parties' discovery obligations under the Federal Rules of Civil Procedure, Local Rules, Stipulated Protocol and Order for Discovery of Electronically Stored Information (ECF No. 315), Stipulation and Order No. 1 Covering Preservation of Electronically Stored Information (ECF No. 411), and Stipulated Protocol and Order for the Search and Culling of Electronically Stored Information (ECF No. 512). Any procedure set forth herein may be modified by written agreement of the Parties where such modification is deemed appropriate to facilitate the timely and economical exchange of data. The Parties agree to use reasonable efforts to comply with the procedures outlined below. Should any Party subsequently determine it cannot in good faith proceed as required by this protocol, the Parties will meet and confer in good faith to resolve any dispute before seeking Court intervention.

C. Privilege Log Exclusions

As previously agreed to by the Parties in the Stipulated Protocol and Order For Discovery of Electronically Stored Information, a privilege log is not required for:

(i) work product created by Counsel, an Agent, or any party at the direction of Counsel, after Marriott publicly announced the Incident on November 30, 2018, or

(ii) any privileged communications generated after Marriott publicly announced the Incident on November 30, 2018, subject to a proper assertion of attorney-client privilege and/or work-product protection where the communications were exchanged between a Party and its Counsel who were acting in their capacity as legal counsel.

If a privileged communication generated after Marriott publicly announced the Incident on November 30,2018, has attachments that are responsive, non-duplicative, and not privileged in and of themselves, it is acceptable to produce those documents as though they were loose documents without any reference to the fact that they were part of a privileged communication. (*See* Stipulated Protocol and Order For Discovery of Electronically Stored Information, ¶ 11(f), ECF No. 315.)

A privilege log is also not required for documents previously provided to regulators that were produced in the Actions pursuant to Judge Grimm's June 12, 2019 Order (Dkt No. 281). Any privilege logs provided to regulators will be reproduced in the Actions.

D. Privilege Log Format

1. The parties shall identify categories (*see* paragraphs D.2a-c *infra*) into which the withheld documents can be arranged to understand and describe (a) the basis for withholding the categories of documents, and (b) the general subject matter of the documents in the category. In addition, the parties may agree that certain categories need not be logged at all, or need not be logged until resolution of a challenge under Paragraph E.2, *infra*.

2. Marriott Defendants identify the initial following categories of documents to be included on their categorical privilege log and reserve the right to propose additional categories for discussion as privilege logging commences and discovery continues:

   a. Marriott to insert categories

   b. Accenture's categories

   c. Plaintiffs' categories

3. The categorical privilege log will consist of the following information regarding the withheld documents and the basis for withholding or redacting the documents:

(i) Category Number: the columns in the categorical privilege log will be numbered in numerical order for ease of identification;

(ii) Category description: Designation of one of the categories listed in Sections 2-4 *supra* or subsequently added by a party;

(iii) Category Date Range: the date of the earliest document and the date of the last document in the category. The Date Range constitutes a subset of the agreed upon relevant date range for discovery in this litigation;

(iv) Category Document Type: list of each type of unique document type included in a category (*e.g.*, email, pdf, PowerPoint);

(v) Specific Custodian(s): list of unique sender(s), recipient(s), and copyee(s) that are Agents, Counsel, or Parties;

(vi) Privilege Description: description of the grounds for withholding the category of Privileged Documents (*e.g.*, prepared at the advice of counsel to assist in anticipated or pending litigation);

(vii) Privilege Justification: basis for withholding the category of documents (*e.g.*, attorney-client privilege, attorney work product);

(viii) Documents Withheld: the total number of documents to which privilege applies in each category; and

(ix) Documents Withheld Including Families: the total number of documents withheld, including the families of those documents, which may not be privileged.

E. Challenge Procedure

1. Following the receipt of a privilege log, a Receiving Party may identify, in writing, the particular category of documents or document that it believes require further

explanation. The Receiving Party shall explain in writing the need for additional information and state precisely each category or document (by document identifier or Bates number) for which it seeks this information.

2. Within fourteen (14) days of such an identification, the producing party must respond to the request by either (i) producing a full log for the requested category of documents, (ii) providing additional information about certain specific documents on any document by document privilege log, or (iii) challenging the request. If a Party challenges a request for further information, the Parties shall follow the protocol by which discovery disputes are heard by Special Master Facciola that was entered by the Court on May 22, 2020 (ECF No. 580).

IT IS SO ORDERED.

Dated: _____ _____

Judge, United States District Court

EXHIBIT O

PARSONS V. KIMPTON
D.E. 84

TERESA C. CHOW, SBN 237694
tchow@bakerlaw.com
MATTHEW PEARSON, SBN 294302
mpearson@bakerlaw.com
BAKER & HOSTETLER LLP
11601 Wilshire Boulevard , Suite 1400
Los Angeles, California 90025-0509
T: 310.820.8800 / F: 310.820.8859

DANIEL R. WARREN, *admitted pro hac vice*
dwarren@bakerlaw.com
THOMAS R. LUCCHESI, *admitted pro hac vice*
tlucchesi@bakerlaw.com
DAVID A. CARNEY, *admitted pro hac vice*
dcarney@bakerlaw.com
DOUGLAS L. SHIVELY, *admitted pro hac vice*
dshively@bakerlaw.com
BAKER & HOSTETLER LLP
127 Public Square, Suite 2000
Cleveland, Ohio 44114
T: 216.620.0200 / F: 216.696.0740

Attorneys for Defendant
KIMPTON HOTEL & RESTAURANT GROUP, LLC

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

ANDREW PARSONS, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

KIMPTON HOTEL & RESTAURANT GROUP, LLC

Defendant.

Case No. 3:16-cv-05387-VC

Hon. Vince G. Chhabria

~~[PROPOSED]~~ ORDER REGARDING PRIVILEGE AND REDACTION DISPUTES

On January 26, 2018, pursuant to the Court's standing order, the parties filed a discovery letter setting forth three discovery disputes regarding privilege and redaction issues. The issues raised by the letter are: (1) whether Kimpton has waived the attorney-client privilege and attorney work-product protection over any document in this case merely by asserting a good-faith affirmative defense in its answer to plaintiff's second amended complaint, which defense does not reference or place at issue advice of counsel; (2) whether the separate, confidential forensics investigation performed by SecureWorks at the direction of counsel following the malware attack on Kimpton's payment card systems is protected from discovery by the attorney-work product doctrine; and (3) whether plaintiff is entitled to discover personal identifying information for individuals who are not parties to this case when this discovery is not necessary for the liability phase of this case. The Court finds Kimpton's positions as set forth in the letter to be well-taken and hereby ORDERS as follows:

1. Kimpton has not waived the attorney-client privilege or attorney work-product protection merely by asserting a good-faith affirmative defense in its answer to plaintiff's second amended complaint. Plaintiff has failed to show how the assertion of this affirmative defense has placed any privileged communications at issue. *See McKeen-Chaplin v. Provident Savings Bank, FSB*, 2015 WL 502697, at *2 (E.D. Cal. Feb. 5, 2015) (finding no waiver because "[d]efendant must support its good faith defense by citing the advice of counsel in order to put it in issue") (collecting cases).

2. The parallel forensics investigation SecureWorks performed on Kimpton's payment card systems following the malware attack is protected from discovery by the attorney-client privilege and the attorney work-product doctrine. Plaintiff has received Mandiant's Final PFI Report and documents related to Mandiant's report but is not entitled to discovery regarding SecureWorks' separate and confidential forensics investigation. *See In re Target Corp. Customer Data Sec. Breach Litig.*, 2015 WL 6777384, at *3 (D. Minn. Oct. 23, 2015) (holding parallel forensics investigation protected from discovery); *Genesco, Inc. v. Visa U.S.A., Inc.*, 302 F.R.D. 168, 190 (M.D. Tenn 2014) (same).

3. Kimpton has appropriately redacted personal information from customer call logs during the liability phase of the case. *Weidenhamer v. Expedia, Inc.*, 2015 WL 7158212, at *4 & n.5 (W.D. Wash. Nov. 13, 2015) (denying motion to compel where "disclosure of the specific PII in this case will involve more than the mere contact information at issue in other cases, but also their travel information").

~~[PROPOSED]~~ ORDER

IT IS SO ORDERED.

Date: February 20 ~~January~~ __, 2018

HON. VINCE G. CHHABRIA
United States District Judge