2021 WL 2660180
Only the Westlaw citation is currently available.
United States District Court, D. Maryland, Southern Division.

IN RE MARRIOTT INTERNATIONAL INC. CUSTOMER DATA SECURITY BREACH LITIGATION
THIS DOCUMENT RELATES TO THE CONSUMER TRACT

MDL NO. 19-MD-2879
|
Signed 06/29/2021

Paul W. Grimm, Judge

I. Introduction

***1** The documents subject to plaintiffs' present challenge to Marriott's claim of privilege were created incident to Marriott's use of an IBM program called Guardium Engagement, which detects database intrusions, and X-Force Red, an IBM vulnerability testing team. Marriott has listed on its privilege log documents pertaining to these programs. Letter of June 7, 2021. According to that letter, the documents being withheld were created for a business purpose and not for provision of legal services to Marriott by BakerHostetler, its counsel.

Plaintiffs claim that documents they have received in discovery indicate that since at least 2011, Marriott (or Starwood) retained IBM to perform what plaintiffs call "cyber-security related products and services." Letter of June 7, 2021, at 1.

According to the plaintiffs' letter, "for many years, Guardium was used by Marriott both for vulnerability scanning and to provide database intrusion and related alerts." Id. at 2. Plaintiffs claim that by late November 2018, however, Marriott "quietly engaged" IBM to assist Marriott "with questions related to Marriott's use of Guardium." Id. at 2. This resulted in a new Statement of Work for IBM's services, which was countersigned by BakerHostetler, Marriott's counsel in this matter. Documents generated by IBM in their Guardium and X-Force Red programs are, according to plaintiffs, not privileged because IBM is providing the same services it has provided Marriott for many years and "manufacturing artificially privileges" between itself and third-party vendors like IBM. They urge Judge Grimm to reject what they call Marriott's machinations and order Marriott to give them the documents claimed to be privileged in the privilege log. Letter of June 7, 2021 at 1-2.

As I understand the plaintiffs' letter, they first demand that Judge Grimm reject Marriott's privilege claim because Marriott has consistently abused its privileges. I shall, therefore, speak first to whether the manner in which Marriott has asserted privileges, in this case, should require Judge Grimm to reject Marriott's most recent claim of privilege for that reason alone. I will then turn to whether the record, in this case, supports the claim that the documents placed in issue by that letter were created for a business purpose.

II. The attempt to defeat the privilege claims.

Plaintiffs accuse Marriott of unethical behavior. They say that (1) Marriott has consistently attempted to create a privilege between itself and its vendors artificially, (2) Marriott has consistently (and improperly) designated nearly every cybersecurity document as privileged, and (3) Marriott engages in sham agreements with its vendors. Letter of June 7, 2021, *passim*. Plaintiffs seek to defeat the claims of privilege because of Marriott's unfair and deceptive assertion of the attorney-client and work-product privileges.

Fed. R. Evid. 501 directs the court to consult the common law in the light of reason and experience in resolving a claim of privilege or, in this case, its abuse. Therefore, the court must ascertain how the common law, as articulated by the state and federal courts, has been applied to the situation.

***2** The Supreme Court's decision in Swindler & Berlin v. United States, 524 U.S. 399 (1998) points the way. The case involved the effort by a Special Prosecutor to obtain the notes an attorney took when he interviewed his client who had died.

The D.C. Circuit balanced the privilege's policy of encouraging clients to be candid with their lawyers against the needs of law enforcement and ordered production of the notes. A dissenting judge concluded the common law rule

—the privilege survived the client's death—should control. Id. at 402-403.

The Supreme Court reversed. It concluded that the appropriate analysis was guided by the common law, i.e., case law that interpreted the privilege. When that case law indicated that the common law rule was that the privilege survived the client's death, it fell to the party seeking to defeat the privilege to show why reason and experience required a different result. Id.

The first question is whether there is common law precedent for the proposition that a court will deny a privilege claim because the claiming party has asserted privilege as Marriott has. There is none.

Plaintiffs claim that Marriott's behavior is nefarious. But that claim misses the forest for the trees. Unquestionably, Marriott has pushed its privilege claims aggressively and to their limits. But it has done so openly by stating its position in its privilege logs and its filings. Plaintiffs, for their part, have challenged those claims, as they are doing now. This court (whether I or Judge Grimm) have then adjudicated the privilege claim. Marriott, like most litigants, has lost some and won some. See, e.g., ECF No. 634. If Marriott is secretly and deviously up to no good, it is not very good at it.

Furthermore, there is certainly no common law precedent for the proposition that Marriott's behavior warrants the sanction of its right to assert that certain documents are privileged. It is certainly true that from the inception of this case, BakerHostetler and one of its partners, Craig Hoffman, have made every effort to create a working environment for its client, its employees, and Marriott's vendors that is insulated from intrusion by the use of attorney-client and work product privileges. Marriott has, however, done so openly and provided the documentation concerning the creation of that environment.

It is equally true that plaintiffs have resisted the creation of that environment as an impediment to discovery. This court then had to consider plaintiffs' challenges to what Marriott has done. In the resulting litigation, Marriott's counsel tried to protect the environment that Hoffman and BakerHostetler have created, and the plaintiffs tried to destroy it with equal aggressiveness.

Thus, all one can say about Marriott and its counsel is that counsel created a work environment that counsel believed was consistent with Marriott's privileges and then defended that environment when plaintiffs challenged it. If that is enough to vitiate the privileges claimed, they have ceased to exist.

I, therefore, find no merit in plaintiffs' claim that the privilege claims asserted by Marriott should be forfeited because of what plaintiffs call Marriott's machinations. Letter of June 7, 2021, at 1.

III. Guardium and X-Force Red

***3** Plaintiffs claim that there is a history of IBM providing services to Marriott and Starwood, including the Guardium and X-Force Red, before discovering the breach in September 2018. The services IBM provided after the breach were the same kind of services IBM provided before the breach. Therefore, IBM did not provide the post-breach services in anticipation of the litigation that flowed from the breach. Instead, they provided the same services that they had provided under earlier agreements for the business purpose of remediating the consequences of the breach. But Marriott and its counsel deviously disguised that reality so that Marriott could claim privileges to defeat discovery into what IBM did. Plaintiffs therefore state:

> Marriott cannot shield its investigation and underlying facts by having its attorneys engage in sham agreements with vendors on its behalf to perform work that was already to occur under pre-existing obligations, which was necessary to investigate and remediate a breach to continue business operations. Nor can it shield routine vulnerability and penetration testing by similarly routing it through counsel.
>
> Here, Marriott needed to uncover the cause of the breach and remediate the breach as a business purpose, *regardless of potential litigation* (and it had already contracted with IBM to perform those services).

Letter of July 7, 2001, at 4 (emphasis original).

Marriott argues to the contrary that BakerHostetler, on behalf of its client Marriott, retained IBM for the Guardium and X-Force Red work in two new engagements, "each of which was

separate from any prior work that IBM had done for Marriott." Letter of June 25, 2021.

The crucial question then becomes why Marriott hired IBM.

IV. Why was IBM hired?
I make the following findings of fact to resolve that question.

FINDINGS OF FACT

Arno Van Der Walt

1. Arno Van Der Walt is the Chief Information Security Officer at Marriott and has held that position since January 2018. Deft. Ex H at para 1. He was responsible for investigating the breach at issue in this case. Id.

2. On September 8, 2018, the defendant Accenture advised Marriott employees that the IBM Guardium application had issued an alert regarding an SQL query to a certain database table. Two days later, Marriott retained BakerHostetler "to conduct an investigation regarding the Guardium event alert to enable BakerHostetler to advise Marriott, initially regarding its potential obligations under contractual obligations and laws, and also in anticipation of payments demands, indemnification demands, and potential regulatory investigations and lawsuits." Id., para 5. Craig Hoffman of that firm "managed and directed the investigation." Id., para 6.

3. According to Van Der Walt, neither Hoffman nor his firm had the tools and knowledge about the Guardium application to investigate it. Id., para 7. Hoffman tried to find a database expert who could help him understand how the Guardium tool worked in relation to a query of a sensitive table in the NDS database without triggering a Guardium alert but could not find one. Id., para 8.

4. Van Der Walt considered hiring IBM to help Hoffman make the query. Id., para 9.

5. On November 15, 2018, Van Der Walt reached out to Jonathan C. Thwaites, an IBM Client Director, and asked him for the name of IBM's best Guardium expert. Id., para 11.

6. Thwaites called back and said that IBM had some people who could help Van Der Walt. Van Der Walt told Thwaites that the potential engagement was at the behest of BakerHostetler and would therefore be privileged "because Marriott needed legal advice." Id., para 12.

7. Van Der Walt explains that although Starwood and Marriott had previously contracted with IBM for services, including licenses for the Guardium application, "there was no pre-existing engagement between IBM and Starwood or Marriott by which IBM provided the services Mr. Hoffman was seeking in November 2018." Id., para 13.

***4** 8. Van Der Walt also notes that there was no business justification for hiring IBM because Marriott's guest reservation system did not use Guardium. Id., para 15.

9. Hoffman recommended to Van Der Walt that Marriott perform a security assessment to review the health of Marriott's mainframe systems to provide legal advice to Marriott. Id., para 16. Van Der Walt, therefore, indicates that BakerHostetler engaged IBM on Marriott's behalf in March 2019 to carry out a security assessment of aspects of Marriott's guest reservation and loyalty databases. Id., para 17.

10. Neither Marriott nor Starwood had previously engaged IBM to provide the types of services called for in the X-Force Red engagement entered into between IBM and BakerHostetler. Id., para 17-18.

John K. Warren

11. John K. Warren is the Vice President & Senior Counsel, Global Compliance, Data Security & Privacy at Marriott. He has submitted an earlier declaration about Marriott's retention of BakerHostetler and its purposes. ECF No. 624 at 1-3. In his newest declaration, he reaffirms that Marriott did not hire BakerHostetler to provide business advice in connection with the data breach. Deft Ex. G para 7. Instead, Marriott hired BakerHostetler to provide "advice regarding contractual and legal obligations and later in anticipation of payment demands, indemnification demands, and regulatory investigations and lawsuits." Id., para 6.

12. On November 14, 2018, Warren received an email from Craig Hoffman of BakerHostetler, which is explained above in paragraph 5-6 that summarizes what Van Der Walt did on November 15, 2021.

13. Warren denies that there was a business purpose for Marriott's engagement of IBM. He indicates, instead, that "the decision to engage a database expert who could help BakerHostetler understand a query of a sensitive table in the NDS database without triggering a Guardium alert was for a legal purpose and an outgrowth of the communications among the Marriott Law Department (myself included) and Marriott's outside counsel at BakerHostetler." Id., para 14. Like Van Der Walt, he indicates that there was no business purpose in engaging IBM to review Guardium's alert on a database that would be retired. In fact, the NDS database was decommissioned and was not used after December 2018.

Craig A. Hoffman

14. Hoffman is a partner at BakerHostetler. He has provided declarations that I have summarized in my prior Reports and Recommendations. ECF Nos. 634 and 707.

15. Hoffman explains that in November 2018, his firm engaged IBM to conduct a narrow and specific investigation to obtain and interpret information regarding the operation of the Guardium application in connection with the NDS database to "assist me in providing legal advice to Marriott in anticipation of adverse regulatory proceedings and litigation." Deft. Ex. F para 3.

16. The investigation of the Starwood network in September 2018 began with an alert by a Guardium application rule. Guardium is an IBM software application with two primary functions: (1) logging database events and (2) issuing alerts when conditions that meet a definite rule occur. One Guardium rule was written to generate an alert when a database administrator account was used to query a table that contained payment card data. Such an alert was issued on September 7, 2018, due to a SQL query seeking the number of rows in the database's "Guest_Master_Profile" table. Id., para 4. On November 13, 2018, an encrypted .rar file was identified on a device in Starwood's network that contained a file named "Guest_Master_Profile.dmp" The .rar file was copied to that device on September 8, 2018. Id., para 5.

***5** 17. Hoffman concluded that he needed a forensic firm to investigate the Guardium aspect of the investigation of the breach. He was unsuccessful and reached out to Marriott's internal legal team to identify a Guardium application expert. As explained above, Hoffman asked Van der Walt if he knew of any such experts, including IBM, since Guardium is an IBM product. Id., para 7. The calls Van der Walt made on November 15, 2018, were therefore done at Hoffman's direction to find the expert Hoffman needed. Id., para 8.

18. Van der Walt then scheduled a "scoping" call with IBM on November 18, 2021. The next morning Hoffman sent an email to IBM telling it to prepare a scope of work "specific to the investigative, analytical items I requested." Hoffman "made it clear to IBM that the statement of work would be a three-party agreement specifying that BakerHostetler was engaging IBM on behalf of Marriott to assist BakerHostetler in providing legal advice to Marriott." Id., para 11.

19. IBM, Marriott, and Hoffman (for BakerHostetler) signed a statement of work in January 2019. He attests that "the expert assistance I received from IBM was not already provided for under a pre-existing contractual relationship between Marriott and IBM." Id., para 13.

20. Hoffman also states that the assessment done by the IBM X-Force Red team was a post-incident security assessment. It has been Hoffman's experience that after a client reveals a data breach, the client should do a security assessment "as part of developing the legal strategy for responding to adverse regulatory investigations and lawsuits." Id., para 19. He, therefore, engaged IBM on behalf of Marriott to conduct the security assessment using X-Force Red. The work was not covered by any pre-existing contract between IBM and Marriott. Id., para 23-24.

The testimony of Alan Booth

21. Alan Booth testified as the Fed. R. Civ. 30(b)(6) witness for IBM.

22. He started to work for IBM in 2002 and is now the client technical leader for the Marriott International Account for IBM. Transcript of deposition of Alan Booth, June 16, 2021, (hereafter "Tr") at 16.

23. Marriott first contacted IBM on or about September 15, 2018, after the discovery of the breach, which is the subject of this case. Tr. at 53. The initial contact was for IBM to bring "Guardium expertise to review some potential suspicious activities." Tr. at 55.

24. IBM, however, did not perform any services based on this request. Although there were meetings and discussions limited to what type of questions IBM should be asking, the process at this point was advisory. Tr. at 55-56. Although IBM was asked to review the Guardium policies, IBM never got them and did not get responses to its communications. Tr. at 56. This changed on November 15, 2018, the date of the next communication between Marriott and IBM.

25. As noted above, this was the day when Van der Walt had his conversation with Thwaites about Hoffman's wanting to hire a Guardium expert. The formal engagement by Marriott of IBM began on November 18. Tr. at 63. The scope of IBM's work was "to investigate some suspicious activity that happened on the NDS database." Tr. at 64.

26. Thus, and beginning on November 18, 2018, Yosef Rozenblit from Guardium lab services was engaged to investigate suspicious activity. Tr. at 70. Asked what forensic activities this gentleman provided, Booth stated: "So, Yosef worked with—under the direction of counsel, worked with Anna Loshkareva [of Marriott] ... and she worked with technicians from Accenture to get him access to the system via WebEx and he was able to investigate and evaluate the system." Tr. at 70. The investigation was not an evaluation of the Guardium environment. Tr. at 71. IBM did not undertake to review the Guardium environment. Instead, IBM "reviewed activities that were recorded by the Guardium system." Tr. at 71-72.

***6** 27. IBM reviewed the logs apparently generated by the work of Rozenblit. Tr. at 81. The logs from the Guardium system showed that IBM looked at that system for a particular date range and observed whether there was suspicious activity from a particular address. Tr. at 85. These logs were from late August to mid-September. Tr. at 86.

Final Conclusion

I find on the basis of my findings that there is no evidentiary support in the record for plaintiffs' assertion that IBM provided the same services it had provided under earlier agreements for the business purpose of remediating the consequences of the breach. The evidence indicates the opposite is true. Hoffman had a precise, limited problem and had his client retain IBM experts to solve it. He did this to assist his client in its response to regulatory authorities and in the litigation (such as this case) that was anticipated. Hoffman also wanted the X-Force Red analysis of the post-breach environment of Marriott's devices because, in his experience, that information might be important to present to regulatory authorities. Every person who provided a sworn statement confirmed the truth and accuracy of what Hoffman said.

Against this wall of evidence, plaintiffs throw a few rocks. They harp on a document in which IBM stated that it does not perform forensic services. Letter of June 7, 2012, at 2. But Booth testified this statement of not performing forensic services was a reference to IBM activity in September 2018, which resulted in nothing. Tr. at 67. It had nothing to do with IBM's engagement and work after November 18, 2018.

Plaintiffs also point to the statements in various documents that IBM evaluated Marriott's system or environment and made recommendations. According to plaintiffs, this proves that what IBM did after November 18, 2018, was simply the same kind of thing it had done for Marriott in the past.

But the use of those words after November 2018, or that IBM may have evaluated a Marriott system or made recommendations concerning it incident to the investigations Marriott sought, does not negate that Marriott retained IBM for a specific and distinct purpose. That an act resulted in a similar occurrence as another act does not mean that the person doing the act had the same purpose each time he did the act. Thus, that the post-November 2018 work yielded a result or results similar to work done before that date cannot negate the universal agreement of the witnesses that Marriott had retained IBM for a specific purpose—to aid Hoffman in his defense of Marriott.

Finding no evidentiary support for plaintiffs' assertions that Marriott is claiming falsely and improperly the privilege to the documents on the log, I recommend that their demand that Marriott provide these documents be rejected.

All Citations

Slip Copy, 2021 WL 2660180

End of Document