UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

IQVIA, INC. and IMS SOFTWARE SERVICES, LTD, Plaintiffs/ Counterclaim Defendants, vs. VEEVA SYSTEMS, INC., Defendant/ Counterclaim Plaintiff.	Case No.: 2:17-CV-00177-CCC-MF **ORDER & OPINION OF THE SPECIAL MASTER**

This matter comes before the Special Master on Plaintiffs-Counterclaim Defendants IQVIA, Inc. and IMS Software Services, LTD's (collectively, "IQVIA") Motion for Sanctions against Defendant-Counterclaim Plaintiff Veeva Systems, Inc. ("Veeva") for Destroying Evidence ("Sanctions Motion"), IQVIA's Motion to Overrule Veeva's Assertion of Privilege over seven clawed back documents and fifty-four other documents ("Privilege Motion"), and IQVIA's Motion for Discovery Regarding Veeva's Apparent Fraud on the Court ("Fraud Motion"). After hearing oral argument on the motions and considering the submissions of the parties, based upon the following, it is the opinion of the Special Master that IQVIA's Sanctions Motion, Privilege Motion, and Fraud Motion are GRANTED in part, as set forth in the following Opinion.

General Factual Background Relevant to all Motions

Both IQVIA and Veeva are companies that sell health care data, which they collect from various sources. In 2007, Veeva began selling to the parties' mutual clients a cloud-based Customer Relationship Management ("CRM") software offering that hosted client data,

including IQVIA's proprietary market research offerings ("Reference Data").[1] Many mutual clients licensed Reference Data from IQVIA and hired Veeva to host it and other data in a CRM system. To facilitate this process, and at those clients' requests, IQVIA granted dozens of licenses – called Third Party Access ("TPA") agreements – that allowed Veeva to host IQVIA Reference Data for this limited purpose.

In 2013, Veeva announced that it was offering a new customer master solution ("Veeva Network"), delivering healthcare provider, organization, and affiliation reference data, a cloud-based software application, and data steward services. To complement Veeva Network and Veeva CRM, Veeva released a reference data product—a compilation of information on healthcare professionals and organizations—called "OpenData." This product would compete directly with IQVIA's OneKey and HCRS reference data offerings. Veeva stated that it was going to use data it was hosting for its clients in CRM to help build Veeva's reference data for Veeva Network. This announcement raised concerns for IQVIA—including that Veeva might improperly use its access to IQVIA Reference Data to build the competing data offering. However, Veeva assured IQVIA that it had stringent protections in place to prevent this from occurring.

The Genentech Incident

In the fall of 2015, in response to IQVIA's concerns and in furtherance of seeking TPA licenses for certain mutual clients, Veeva agreed to an independent audit by Ernst & Young ("E&Y Audit"). Veeva was provided a Pre-Audit Questionnaire in advance of the audit. To

[1] IQVIA licenses numerous data offerings that include key attributes on healthcare professionals, healthcare organizations, and/or the complex web of affiliations that link them together. IQVIA's primary reference data offerings are currently marketed under the name "OneKey." However, IQVIA has also marketed U.S. reference data offerings under other names such as: IMS HCRS (Healthcare Relationship Services), IMS HCOS (Healthcare Organization Services) and IMS HCPS (Healthcare Professional Services). Other IQVIA offerings—including U.S. sales and prescription information services offerings marketed under the names DDD and Xponent, respectively—also include proprietary IQVIA reference data attributes. For simplicity's sake, this Order and Opinion refers to these IQVIA offerings collectively as "Reference Data."

respond to the questionnaire, Veeva conducted an internal investigation of its operations during which it learned of a "data corruption" problem. The "data corruption" problem originated from a company – AdvantageMS ("AMS") – that Veeva had acquired in 2013. AMS's customer, Genentech, provided a dataset to AMS for data-research and data-improvement services. The Genentech dataset included IQVIA records, which became accessible to Veeva pursuant to a TPA license. In September 2015, Veeva discovered that because of a configuration error in a data table storing Genentech's address data, IQVIA address records were inadvertently included as a source in Veeva's "best address" algorithm to verify address records in OpenData (the "Genentech Incident"). Further, the database storing those records was viewable by Veeva's OpenData data stewards, who were tasked with improving and maintaining Veeva OpenData.

After discovering the Genentech Incident, Veeva twice rescheduled the E&Y Audit. Veeva employees then engaged in a series of internal communications to determine the extent of the "data corruption" and the business response thereto. Having concluded that the Genentech incident was "minor," Veeva decided against publicly disclosing the incident. The E&Y Audit ultimately occurred and the parties continued their business relationship.

The Shire Incident

Thereafter, in April 2016, Veeva obtained a data extract from mutual customer Shire Pharmaceuticals ("Shire") for a Data Report Card ("DRC"), which resulted in unauthorized access to IQVIA data (the "Shire Incident"). DRCs are tools by which data vendors educate potential data customers on the accuracy of their data. Veeva's DRC process worked as follows: Veeva obtained a potential customer's data extract directly from that company or from Veeva's CRM system. In so doing, that company affirmed its right (under licensing agreements or otherwise) to authorize Veeva's use of the extract to conduct a DRC. Veeva then generated a

comparison between the extract and OpenData. The exercise identified inaccuracies or omissions in customer data that OpenData could cure.

In this instance, Veeva obtained authorization from Shire's IT department to generate the DRC, and confirmation that Shire had all necessary rights to provide the information to Veeva for the purpose of performing the analysis. However, Shire did not have a TPA license in place and realized that it had inadvertently authorized use of an extract containing IQVIA data without IQVIA's authorization. Shire informed Veeva that it wished to terminate the DRC process. Veeva obliged and deleted the Shire extract from its systems. Shire then informed IQVIA about the incident and Veeva confirmed to IQVIA that it had deleted the Shire data and the data did not contribute to Veeva's OpenData product.

On January 10, 2017, IQVIA filed the instant lawsuit. (ECF No. 1.) In its Complaint, IQVIA alleges that Veeva stole IQVIA's confidential and proprietary information and used it to develop and improve its own competing products and services. (*Id.* at ¶ 1.) Specifically, IQVIA contends that Veeva improperly gained access to IQVIA data through the use of DRCs. (*Id.* at ¶¶ 119-129.)

James Kahan E-mails

Veeva employee James Kahan, Senior Director of Veeva OpenData, has been identified as a key witness in this matter. In June 2019, the Special Master ordered Veeva to produce Kahan's custodial documents, which Veeva did in September 2019. However, the production was missing e-mails that coincided with the timeframe in which he served as the senior manager responsible for Veeva OpenData, specifically, January 2014 through May 2015. Initially, Veeva indicated that Kahan had deleted his e-mails. However, Kahan denied this at his deposition and testified that he does not know who deleted his e-mails and only learned they were deleted in

preparation for his deposition. Veeva insists that it is unaware who deleted Kahan's e-mails or when they were deleted, other than them being deleted in the ordinary course, pre-litigation.

EUStage

When Veeva began building OpenData in Europe in 2015, it designed a two-part computer system in which Veeva employees would work: (1) an intermediate OpenData database; and (2) a final OpenData database. Each database was stored in a separate "instance" of Veeva Network, Veeva's cloud master data management software. The intermediate OpenData database was stored in an instance called "EUStage." This was the "staging" environment where the database was actually built. The final OpenData database was stored in a separate production "instance" called "EUMaster." Each "instance" has its own audit trail, which tracks where the data contained within the instance originated. On August 10, 2018, Veeva deleted EUStage.

Google Drive

Google Drive is one of the central repositories in which Veeva stores and manages documents. In March 2019, after deposing Veeva employee RJ Johnston, IQVIA requested certain documents that Johnston had created or accessed on Google Drive. Veeva responded that it no longer had the documents because they had been deleted. IQVIA filed a motion to compel Veeva to produce all responsive Google Drive documents and respond to IQVIA's questions about when the Google Drive documents were deleted. In opposing the motion, Veeva submitted a declaration from a member of its IT department, in which it indicated that the documents were deleted before December 9, 2016, prior to IQVIA's filing of the instant lawsuit. Thereafter, in November 2019, Veeva's corporate designee on deletion topics testified that Veeva did not begin preserving documents stored on Google Drive until "mid-January" 2017. Later, Veeva indicated that it did not begin preserving Google Drive documents until April 25, 2017.

Privilege Motion

I. Arguments of the Parties

A. IQVIA's Arguments

IQVIA argues that Veeva has improperly clawed back seven documents on the basis of privilege. IQVIA contends that these documents are neither privileged nor protected in any manner, and instead, they provide contemporaneous evidence of Veeva's wrongdoing both before and after this lawsuit commenced. First, IQVIA contends that Veeva clawed back two versions of a spreadsheet (referred to as the "DataDestroyed Spreadsheet") created by its employee, RJ Johnston, that is a contemporaneous record of Veeva's systemic efforts to destroy incriminating evidence in the months after IQVIA filed this lawsuit. Second, IQVIA claims that Veeva clawed back three other documents that were created in the fall of 2015 (referred to as the "Cover-Up Documents"), on the eve of the E&Y Audit, which demonstrate actions taken by Veeva's executives to cover up the fact that Veeva had been "programmatically" stealing IQVIA data. Third, IQVIA contends that Veeva clawed back two other documents – (1) a non-privileged e-mail between a Veeva employee and his wife, and (2) a Shire Incident Report that Veeva waited to claw back for over seven months after it was used by IQVIA at the deposition of a Veeva witness. Finally, IQVIA contends that there are fifty-four other documents in Veeva's privilege log that relate to the Cover-Up Documents, which are not privileged. IQVIA argues that even if the above-referenced documents are privileged, they are subject to the crime-fraud exception and should be produced.[2]

[2] IQVIA includes these seven documents with its motion papers, labeled Exhibits A through G, respectively. With its opposition, Veeva produced the same exhibits, in a slightly different order, labeled as Exhibits A-1 through A-7. Veeva also provided the Special Master with the fifty-four other documents that IQVIA challenges, labeled as Exhibits A-8 through A-61. For ease of reference, and consistency throughout the opinion, the Special Master will rely on Veeva's labels for the exhibits, unless expressly noted otherwise.

With respect to the DataDestroyed Spreadsheet, IQVIA contends that Veeva produced the first version of the document on August 8, 2019. Thereafter, on November 21, 2019, Veeva clawed back the document, after IQVIA listed it as a topic in a Rule[3] 30(b)(6) deposition notice concerning Veeva's purported improper deletion of relevant evidence. IQVIA argues that the DataDestroyed Spreadsheet appears to be a contemporaneous record of Veeva's calculated and ongoing efforts to destroy evidence after IQVIA filed its lawsuit. Specifically, it contains a number of sheets that identify clients that licensed data from IQVIA. The document then indicates whether the data that Veeva obtained from these customers was "Destroyed" ("DataDestroyed (Y/N/U)") from several locations in Veeva's systems including "HDM" (a Veeva environment that contributes to OpenData), "EGNYTE" (cloud storage), and "Internal E-mail." In many cases, the answer is "Y," which IQVIA contends shows that Veeva had destroyed the data from the location in question. IQVIA further argues that in many cases, the DataDestroyed Spreadsheet expressly notes that the deleted data in question relates to a "DIR" or "Data Insight Report." In this lawsuit, IQVIA alleges that Veeva used DIRs as a pretext to persuade customers to grant Veeva unauthorized access to proprietary IQVIA data. IQVIA further argues that the DataDestroyed Spreadsheet expressly notes that, in many cases, Veeva "***PURGED***" data related to these DIRs. Furthermore, the DataDestroyed Spreadsheet contains comments suggesting that deletions were ongoing or in progress. IQVIA contends that the DataDestroyed Spreadsheet also demonstrates that Veeva made false statements to IQVIA and the Court about certain evidence being deleted before litigation, when in fact, the DataDestroyed Spreadsheet confirms that these deletions occurred after litigation commenced. IQVIA further contends that there is a second version of the DataDestroyed Spreadsheet, that Veeva clawed back on January 31, 2020, which is similar to the first spreadsheet, but also records data extracts

[3] All references to a Rule are references to a Federal Rule of Civil Procedure.

that Veeva acquired in April 2017, showing that Veeva's deletion campaign continued well beyond the filing of the Complaint. Veeva admits that the DataDestroyed Spreadsheet was created in February 2017, after litigation commenced, at the direction of counsel. Thus, IQVIA argues, the DataDestroyed Spreadsheet is a record of spoliation, is subject to the crime-fraud exception, and cannot be withheld on privilege grounds.

With respect to the Cover-Up Documents, IQVIA argues that they are not privileged because they were not necessary for the provision of legal advice or prepared primarily for the purpose of litigation. Rather, IQVIA contends, the Cover-Up Documents were created for business purposes, and even if they did involve the provision of legal advice, the crime-fraud exception applies because the documents were created in support of an attempt to spoliate evidence and defraud IQVIA into granting Veeva TPA licenses based on deception and lies. The first of the Cover-Up Documents is what IQVIA refers to as Veeva's "Communication Plan" for the data corruption problem (Exhibit A-4),[4] which Veeva produced on October 19, 2018, and clawed back on November 13, 2019. IQVIA argues that the document was prepared at a time when Veeva management was going to admit that it had been unlawfully accessing IQVIA data and contemplates a public relations campaign for dealing with the fallout from its admission. The second of the Cover-Up Documents is the e-mail chain to which the Communication Plan is attached (Exhibit A-5.) It was also produced on October 19, 2018, and clawed back on November 13, 2019. The e-mail chain is between three Veeva executives, and notes that the attached Communication Plan is part of a "recommendation for [CEO Peter Gassner's] review." The e-mail chain copies Veeva's in-house counsel, but, according to IQVIA, subsequent communications indicate that Veeva's in-house counsel was not expected to or planning on

[4] Veeva refers to this document as an earlier version of the OpenData Data Corruption Memo.

providing legal advice in connection with the document. The third of the Cover-Up Documents is referred to as the "OpenData Data Corruption Memo." (Exhibit A-3.) IQVIA argues that most of this memo is devoted to Veeva's "Go Forward Plan" for addressing the misuse of IQVIA data in connection with the Genentech Incident. IQVIA further argues that the Executive Section of the OpenData Data Corruption Memo outlines the non-legal reasons for the document's creation: "The following document provides the plan to address the architectural and organizational/policy issues as well as defines the potential risk and approach to communication plan/approach/timeline to the various parties, both internal and external." IQVIA also argues that the e-mail chain, to which the OpenData Data Corruption Memo is attached,[5] further indicates the non-legal purpose of the document. The e-mail is between Veeva executives, and although it copies Veeva's in-house counsel, it is described as containing "the plan to fix, communicate, messaging, timing and potential risk" for review by the management team. IQVIA argues that merely copying an attorney on an e-mail or a document does not make it privileged.

As it relates to the fifty-four other documents in Veeva's privilege log that IQVIA contends are improperly withheld on the basis of privilege ("Other Privileged Documents"), IQVIA argues that they were created during the same time period (the run-up to the E&Y Audit) and pertain to the same subject matter at issue as the documents that Veeva clawed back. Indeed, some of the documents appear to be other versions of the OpenData Data Corruption Memo. Thus, IQVIA requests that the Special Master compel production of these Other Privileged Documents, or conduct an *in camera* review of them and then order production of any documents improperly withheld.

IQVIA further argues that even if any of the aforementioned documents contains legal advice, they are discoverable under the crime-fraud exception. IQVIA contends that the crime-

[5] *See* IQVIA Exhibit O. Veeva produced this document with minor redactions.

fraud exception applies for two reasons: (1) the communications were part of Veeva's scheme to spoliate evidence; and (2) the communications were made in furtherance of Veeva's attempt to defraud IQVIA into granting TPA licenses. IQVIA claims that the OpenData Data Corruption Memo is a contemporaneous record of Veeva's spoliation of evidence during the pendency of this litigation. IQVIA argues that in advance of the E&Y Audit, Veeva was sent a Pre-Audit Questionnaire that asked for a "complete listing of all Data in your possession, or to which you have had access during the Review Period." IQVIA contends that the Pre-Audit Questionnaire prompted Veeva to conduct an internal investigation, which revealed that Veeva had been misappropriating IQVIA data. However, IQVIA argues that Veeva created the above-referenced documents after receiving the Pre-Audit Questionnaire, but before providing its response thereto. IQVIA further argues that Veeva's response to the Pre-Audit Questionnaire did not disclose highly material information in an effort to induce IQVIA to grant TPA licenses to Veeva. Thus, according to IQVIA, the above-referenced documents were created in furtherance of Veeva's commission of a fraud, and to the extent they may be privileged, they are subject to the crime-fraud exception.

Finally, IQVIA contends that Veeva also improperly clawed back a September 25, 2015, e-mail between Veeva employee Tim Slevin and his wife, Susan Slevin (the "Slevin E-mail") and the Shire Incident Report.[6] The Slevin E-mail is a draft e-mail that Veeva employee, Tim Slevin, prepared to Veeva CEO, Robert Gassner, and sent to his wife, Susan Slevin, for feedback. IQVIA argues that this document is not privileged because it contains the thoughts of a business person. Even if it were privileged, IQVIA argues that any claim of privilege was waived by Mr. Slevin because he sent the allegedly privileged communication to a third-party, his wife.

[6] Veeva has since withdrawn its claim of privilege and has produced the Shire Incident Report.

B. Veeva's Arguments

Veeva argues that all of the documents that are the subject of IQVIA's Privilege Motion are privileged documents because they are or include legal advice from Veeva's in-house counsel, communications made for the purpose of obtaining legal guidance, and material prepared or retrieved at the direction of counsel. Veeva argues that the DataDestroyed Spreadsheet[7] was prepared at the instruction of Veeva's in-house counsel and that IQVIA misunderstands the spreadsheet. Specifically, Veeva contends that the DataDestroyed Spreadsheet was not created to track deletions, but rather, was intended to capture which datasets Veeva still retained. Veeva further argues that the Cover-Up Documents are related to the investigation of a "minor database-configuration error involving a negligible number of IQVIA address records" and are not proof of a spoliation scheme as asserted by IQVIA. In addition, Veeva contends that the Slevin E-mail is privileged because it is an e-mail request for legal advice that merely copies a spouse, which does not break the privilege. Veeva further contends that IQVIA's arguments with respect to the remaining challenged documents are insufficient. Veeva submits the Other Privileged Documents to the Special Master for *in camera* review. Veeva argues that these documents reflect guidance from Veeva's in-house counsel regarding the company's obligations under TPA licenses, legal analysis of Veeva's internal procedures, legal advice regarding data storage and confidentiality, and documents or materials circulated to counsel for these and other privileged purposes, and are therefore protected from disclosure.

Veeva argues that both versions of the DataDestroyed Spreadsheet are protected by the attorney-client privilege because they were created at the direction of counsel. Veeva contends that it used DRCs in connection with the marketing of OpenData, which is a competitive product

[7] Veeva refers to the DataDestroyed Spreadsheet as the "Data Tracking Spreadsheet." To avoid confusion, the Special Master refers to it as the "DataDestroyed Spreadsheet," as set forth in the moving papers, with the understanding that this is not an official title of the document, but rather, a label provided by the moving party.

to IQVIA's OneKey. Veeva further contends that in connection with the DRCs, a potential OpenData customer would grant Veeva access to a sample of its data ("data extract"), which Veeva would use to run a comparison between the customer's data extract and OpenData. Veeva further contends that in connection with the DRC, Veeva would require the customer to certify that it had the right to grant Veeva access to the data extract for DRC purposes. Veeva argues that after IQVIA filed this lawsuit in January 2017, which accused Veeva of using DRCs to steal IQVIA's proprietary information, Veeva's in-house counsel instructed employees "to prepare a spreadsheet documenting (1) customers for whom Veeva had generated DRCs and (2) the status of data received as part of the DRC process." (Declaration of Jonathan W. Faddis in Opposition to the Privilege Motion ("Faddis Declaration") at ¶ 20.) Veeva claims that the purpose of the DataDestroyed Spreadsheet was not to track deletions, but rather, to track and catalog data collected from customers that received a DRC so that Veeva's in-house counsel could evaluate IQVIA's lawsuit and assess any legal obligations Veeva had to customers and IQVIA regarding data obtained as part of the DRC process. Veeva contends that IQVIA does not dispute that the DataDestroyed Spreadsheet is privileged, as it contains a notation that it was prepared at the direction of counsel, but rather, IQVIA argues that the spreadsheet is proof of spoliation and subject to the crime-fraud exception. Veeva disputes that the DataDestroyed Spreadsheet constitutes a fraud on the Court or is evidence of spoliation. Veeva further argues that IQVIA fails to prove that any relevant data extracts reflected in the DataDestroyed Spreadsheet were deleted after it filed this lawsuit. Veeva contends that it, in fact, produced many of the data extracts referenced in the DataDestroyed Spreadsheet during discovery, thus defeating IQVIA's claims that the extracts were fraudulently deleted. Veeva also argues that apart from actually showing that the data extracts were deleted, IQVIA fails to demonstrate which, if any, of the data

extracts are relevant to this litigation. Veeva contends that the data extracts of the six Veeva DRC customers that IQVIA mentions in its moving papers are irrelevant because none of the extracts contained IQVIA data. Furthermore, Veeva claims that there is no evidence that Veeva's in-house counsel instructed Veeva employees to create the DataDestroyed Spreadsheet to further an unlawful act, which is required for the crime-fraud exception to apply.

With respect to the Cover-Up Documents,[8] Veeva contends that they relate to "an inconsequential database-configuration error that involved a small number of records stored for one of Veeva's customers, Genentech, Inc., pursuant to a TPA signed by IQVIA [(the Genentech Incident).]" (Veeva Opp. Br. at p. 10.) Veeva further contends that the Cover-Up Documents – which include: (1) the OpenData Data Corruption Memo (Exhibit A-3); (2) a prior, partial draft of the OpenData Data Corruption Memo (Exhibit A-4); and (3) a cover e-mail attaching the OpenData Data Corruption Memo (Exhibit A-5) – as well as twenty-five of the Other Privileged Documents, are all privileged because they specifically sought legal advice. Furthermore, Veeva argues that its in-house counsel did in fact provide legal advice about the Cover-Up Documents. Veeva argues that the fact that the Cover-Up Documents may have been made for a business purpose and were circulated amongst non-lawyers does not vitiate the attorney-client privilege where they were sent to in-house counsel for the purpose of obtaining legal advice. Veeva contends that any business strategy in connection with these documents was "infused with legal concerns" and that Veeva's in-house counsel's legal advice "informed Veeva's decision-making process[.]" Moreover, Veeva argues that the crime-fraud exception does not apply because the Cover-Up Documents were not created to further any alleged crime or fraud. Veeva claims that it had no reason to anticipate litigation at the time the Cover-Up Documents were created, and

[8] The Special Master notes that Veeva refers to these documents as the "Genentech Documents." The Special Master will use the term set forth in the moving papers – "Cover-Up Documents" – for consistency.

therefore, was under no obligation to preserve evidence. Veeva also claims that it did not commit any fraud in connection with responding to the Pre-Audit Questionnaire, which asked whether Veeva obtained IQVIA data "with the *intention or expectation* that the data may be used in *Veeva Network*." (Veeva Opp. Br. at p. 18.) Veeva argues that Genentech was not a Veeva Network customer, its dataset was stored in a legacy AMS database that Veeva had acquired years earlier, and the Pre-Audit Questionnaire specifically asked whether Veeva obtained data intentionally. Veeva contends that the Genentech Incident involved inadvertent access to IQVIA data.

Veeva further contends that the redacted portion of the Slevin E-mail is privileged because it contains an explicit request for legal advice from counsel. Veeva argues that the document does not lose its privilege because Mr. Slevin sent it to his spouse and intended to send it to Veeva's CEO, Peter Gassner. Veeva contends that Mr. Slevin sought advice from his wife and Mr. Gassner in furtherance of his request for legal advice.

Finally, Veeva argues that IQVIA's motion contains little meaningful discussion with respect to the Other Privileged Documents, which are lumped into one appendix. Veeva contends that these documents are all privileged and fall into one of four categories: (1) legal advice regarding TPA agreements (12 documents – Exhibits A-8 through A-19); (2) legal advice regarding the E&Y Audit (12 documents – Exhibits A-20 through A-31); (3) legal advice relating to the Genentech Incident (25 documents – Exhibits A-32 through A-56); and (4) conversations among non-lawyer employees (5 documents – Exhibits A-57 through A-61). With respect to the first category – legal advice regarding TPA agreements – Veeva contends that these twelve documents reflect in-house counsel's legal advice regarding TPA agreements, requests for such advice, draft contractual terms, and other material assembled at counsel's

instruction to help him provide legal advice, and are thus protected by the attorney-client privilege. With respect to the second category – legal advice regarding the E&Y Audit – Veeva contends that its in-house counsel negotiated the terms of the audit, provided legal advice regarding Veeva's preparation for and participation in the audit, and asked employees to assemble materials for legal review. Thus, Veeva contends, these documents are protected by the attorney-client privilege. Veeva also argues that these documents reflect "intracorporate communications made during an internal investigation that Veeva undertook to prepare for the E&Y [A]udit" and that the attorney-client privilege "protects communications made during an internal investigation to assess legal compliance[.]" The third category – legal advice relating to the Genentech Incident – contains twenty-five documents that are cover e-mails, related documents, or drafts of the OpenData Data Corruption Memo. Veeva contends that just as the Cover-Up Documents are privileged, so too are these drafts and cover communications. Finally, the fourth category of documents – conversations among non-lawyer employees – contains five documents that Veeva contends are privileged because they contain: (1) discussion of factual material collected for counsel; (2) factual communications to help counsel provide legal advice; and (3) requests for legal advice from counsel.

Veeva also argues that IQVIA's motion should be dismissed because it is procedurally deficient as IQVIA failed to first meet and confer with Veeva regarding the subject matter of the motion, and IQVIA's challenges to the clawed back documents are untimely under the Discovery Confidentiality Order ("DCO"). Veeva contends that under the DCO, challenges to a party's claim of privilege must be asserted within a "reasonable time." Veeva further contends that IQVIA waited more than three months before filing a motion to compel, which Veeva contends is not a reasonable amount of time.

C. IQVIA's Reply

In reply, IQVIA argues that Veeva is unable to explain the futuristic language contained in the DataDestroyed Spreadsheet, specifically directing Veeva personnel to find and purge data. IQVIA further argues that Veeva does not dispute that the DataDestroyed Spreadsheet was created after litigation began. IQVIA contends that it need not produce evidence that Veeva committed a crime or a fraud, but rather, it need only show a "reasonable basis to suspect" that the DataDestroyed Spreadsheet was "used in furtherance" of spoliation that Veeva was committing or intending to commit. (IQVIA Reply Br. at p. 5.) IQVIA argues that the self-serving affidavit from Veeva's in-house counsel, in which he contends that the DataDestroyed Spreadsheet was created to help him provide legal advice, without any corroborating contemporaneous evidence, is inconsistent with the spreadsheet itself, as well as Veeva's production and earlier sworn statements by Veeva's counsel. For example, IQVIA contends that Veeva indicated in its July 2018 answers to IQVIA's interrogatories that a certain customer data extract was deleted prior to litigation, but now claims in its opposition to the Privilege Motion that the DataDestroyed Spreadsheet shows that such data was identified and the custodian was instructed not to delete it. IQVIA also contends that the fact that Veeva produced some data extracts does not render the deletion of other data extracts insignificant. IQVIA notes that at least nineteen of the data extracts listed in the DataDestroyed Spreadsheet were deleted and not produced. Furthermore, IQVIA argues that there are eight extracts referenced in the DataDestroyed Spreadsheet that Veeva did not even identify in its interrogatory responses. Thus, IQVIA argues that Veeva's claim that the DataDestroyed Spreadsheet was created to assist counsel in identifying data extracts that remained in Veeva's possession is insincere.

IQVIA argues that Veeva concedes that the Cover-Up Documents were not prepared by or for an attorney. Rather, IQVIA argues, Veeva admits they were prepared by a non-lawyer, with assistance from other business executives, and contain business recommendations meant for Veeva's CEO. IQVIA further argues that these concessions, along with the OpenData Data Corruption Memo's own clear statement of its principally business purpose show that the document does not meet the predominantly legal standard for privilege to apply. IQVIA contends that Veeva's brief and supporting affidavits further confirm that the Cover-Up Documents are not privileged because Veeva's in-house counsel contends they were prepared "in part" to help him assess Veeva's legal risk, yet Veeva provides no contemporaneous record of in-house counsel's review of the documents for that stated purpose. IQVIA further contends that even if the Cover-Up Documents had mixed legal and business purposes, the legal purposes would have to predominate over the business purpose for privilege to apply, which IQVIA contends is not the case. IQVIA argues that Veeva is attempting to claim privilege over all documents relating to the Genentech Incident because Veeva's in-house counsel was involved in Veeva's investigation and handling of that issue. IQVIA also distinguishes the Special Master's ruling upholding IQVIA's claim of privilege over draft PowerPoint presentations that were sent to counsel for review. First, IQVIA argues that it provided contemporaneous evidence actually demonstrating that the draft presentations were in fact sent to in-house counsel for his legal advice. Second, IQVIA contends that it produced the final versions of the draft presentations, something that Veeva refuses to do.

IQVIA maintains that the Cover-Up Documents were created in furtherance of actual and attempted fraud on the Court and IQVIA. IQVIA argues that the OpenData Data Corruption Memo itself contemplates litigation when it identifies the "risk" to Veeva arising from the "data

corruption" issue being that "[IQVIA] will file a lawsuit against Veeva for damages[.]" Thus, Veeva's claims that it did not anticipate litigation at the time the memo was created are disingenuous. Furthermore, IQVIA contends that Veeva had taken the position that certain documents created in the fall of 2015 were protected by the work-product privilege as they were prepared in anticipation of litigation. IQVIA argues that Veeva then backtracked and withdrew these privilege assertions only after it realized that they would lead to the conclusion that Veeva spoliated evidence. IQVIA contends that Veeva relies only on self-serving statements made by Veeva's in-house counsel, that he did not anticipate any litigation, which are unsupported by any other contemporaneous evidence. Furthermore, IQVIA argues that it is not Veeva's in-house counsel's subjective belief that governs, but rather, whether a reasonable party would have foreseen litigation. IQVIA also argues that Veeva has placed in issue when it anticipated litigation by representing to the Court that it did not anticipate litigation until January 2017. Thus, IQVIA maintains that Veeva should not be able to use that factual assertion as both a sword and a shield. Finally, IQVIA argues that the Cover-Up Documents must be produced, even if they contain legal advice, because any such advice was provided in furtherance of Veeva's attempt to hide its theft of IQVIA's intellectual property from third-party auditors and fraudulently induce IQVIA into granting TPA licenses permitting Veeva to load the intellectual property into Veeva's cloud software products. Specifically, IQVIA argues that the Cover-Up Documents were created for an "OPS meeting" of Veeva's senior leadership, during which, in reliance on these materials, Veeva decided to engage in a cover-up. Therefore, IQVIA maintains that the documents were used to commit fraud and are discoverable under the crime-fraud exception.

As it pertains to the Other Privileged Documents, IQVIA argues that the twenty-five documents (A-32 to A-56) related to the OpenData Data Corruption Memo are discoverable because they are not predominantly legal communications and were created in furtherance of a fraud on the Court and attempted fraud on IQVIA. IQVIA contends that Veeva's argument that these documents are privileged because they are drafts or cover communications relating to the OpenData Data Corruption Memo is a conclusory assertion and insufficient to meet Veeva's burden. With respect to document A-61 ("Slevin's Way Forward Path Analysis"), IQVIA argues that it was prepared for the OPS meeting of Veeva executives, there is no evidence that any attorney actually attended that meeting or provided legal advice at that meeting, and even if an attorney did attend that meeting, it does not make the document privileged. With respect to the chats (A-57 through A-60), IQVIA argues that any gathering of information by these employees was in furtherance of a business purpose and not for legal review. IQVIA argues that the remaining documents (A-8 through A-31), which purportedly contain legal advice regarding either the E&Y Audit or Veeva's obligation under TPA agreements, should be produced to the extent they were used in furtherance of the fraud set forth above. IQVIA also argues that the Slevin E-mail is not privileged because it was a business document that Slevin shared with his wife for his own personal purposes. IQVIA further argues that there is no attorney on the e-mail chain and no request for legal advice.

Finally, IQVIA argues that its motion is procedurally proper as it made multiple attempts to obtain further information about Veeva's privilege assertions, but Veeva failed to provide additional information. With respect to the Cover-Up Documents, IQVIA contends that it challenged Veeva's privilege assertions over these documents in mid-November 2019. IQVIA further contends that the parties discussed a meet and confer for the week of November 25, 2019,

but after the deposition of Veeva's 30(b)(6) witness, Josh Faddis, on November 24, 2019, it became apparent that Veeva would not provide any meaningful information concerning its privilege claims. Thus, IQVIA contends, the meet and confer would have been futile. Finally, IQVIA argues that its delay (from 30 to 90 days) in challenging Veeva's clawed back documents is reasonable in light of the winter holiday and the extensive discovery in which the parties were engaged at the time.

II. Applicable Law

Evidentiary privileges are an exception to the general rule that relevant evidence is admissible. *Rhone-Poulenc Rorer Inc. v. Home Indem. Co.*, 32 F.3d 851, 862 (3d. Cir. 1994). Privileges forbid the admission of otherwise relevant evidence when certain interests that the privileges are thought to protect are considered more important than the interests served by the resolution of litigation through full disclosure of all relevant facts. *Id.* "The privilege forbidding the discovery and admission of evidence relating to communications between attorney and client is intended to ensure that a client remains free from apprehension that consultations with a legal advisor will be disclosed." *Id.* The privilege encourages the client to reveal confidences to the lawyer necessary for the lawyer to provide advice and representation. *Id.*; *see also Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981) (holding that the purpose of the attorney-client privilege is "to encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice."). Thus, the attorney-client privilege protects (1) communications (2) between "privileged persons" (3) made in confidence (4) intended to receive or give legal assistance. *In re Teleglobe Commc'ns Corp.*, 493 F.3d 345, 359 (3d Cir. 2007), as amended (Oct. 12, 2007) (quoting Restatement (Third) of the Law Governing Lawyers § 68 (2000)). The attorney-client privilege extends to

corporations which must act through agents, including their officers and employees. *Leonen v. Johns-Manville*, 135 F.R.D. 94, 98 (D.N.J. 1990).

Because the privilege obstructs the truth-finding process, it is construed narrowly, and "'protects only those disclosures – necessary to obtain informed legal advice – which might not have been made absent the privilege.'" *Westinghouse Elec. Corp. v. Republic of the Philippines*, 951 F.2d 1414, 1423-24 (3d Cir. 1991) (quoting *Fisher v. United States*, 425 U.S. 391, 403 (1976)). Thus, for a communication to be protected, it must be made to an attorney for the express purpose of obtaining legal advice. *Fisher*, 425 U.S. at 403. Business and personal advice are not protected by the privilege. *Claude P. Bamberger Inter. Inc. v. Rohm and Haas Co.*, 1997 WL 33768546, at * 2 (D.N.J. Aug. 12, 1997) (citing *United States v. Davis*, 636 F.2d 1028, 1044 (5th Cir. 1978), *cert. denied*, 454 U.S. 862 (1981)). Where a communication contains both legal and business advice, the attorney-client privilege will apply only if the primary purpose of the communication was to aid in the provision of legal advice. *Id.* (citing *Hercules, Inc. v. Exxon Corp.*, 434 F.Supp. 136, 147 (D.Del. 1977)). Just as a litigant may not shield non-privileged information from discovery by combining it with legal advice, a litigant cannot cloak business information in privilege by involving an attorney in the communication of business matters. *United States v. Rockwell Int'l*, 897 F.2d 1255 (3d Cir. 1990) ("The sine qua non of any claim of privilege is that the information sought to be shielded is legal advice."); *Yang v. Reno*, 157 F.R.D. 625, 636 (M.D. Pa. 1994) (holding that the attendance of an attorney at meeting called by the attorney did not render everything said or done at that meeting privileged, rather, for the privilege to apply, the communication must have related to the acquisition or rendition of professional legal services).

In addition, the attorney-client privilege does not apply simply because a statement was made by or to an attorney. *Nanticoke Lenni-Lenape Tribal Nation v. Porrino*, 2017 WL 4155368, at *3 (D.N.J. Sept. 19, 2017). Merely copying an attorney on an e-mail does not, in and of itself, make the e-mail privileged. *In re Human Tissue Products Liability Litigation*, 255 F.R.D. 151, 164 (D.N.J. 2008); *Andritz Sprout-Bauer, Inc. v. Beazer East, Inc.*, 174 F.R.D. 609, 633 (M.D. Pa. 1997) ("What would otherwise be routine, non-privileged communications between corporate officers or employees transacting the general business of the company do not attain privileged status solely because in-house counsel or outside counsel is 'copied in' on correspondence or memoranda") *United States Postal Serv. v. Phelps Dodge Ref. Corp.*, 852 F.Supp. 156, 163 (E.D.N.Y. 1994) ("A corporation cannot be permitted to insulate its files from discovery simply by sending a 'cc' to in-house counsel"). "'To rule otherwise would allow parties to evade the privilege limitations by sending copies of every company-generated e-mail to the company's attorney so as to protect the communication from discovery, regardless of whether legal services were sought or who the other recipients of the e-mail were.'" *In re Human Tissue Products Liability Litigation*, 255 F.R.D. at 164 (quoting *In re Avantel, S.A.*, 343 F.3d 311, 321 (5th Cir. 2003)). If a privileged document has attachments, each attachment must individually qualify for the privilege. "Merely attaching something to a privileged document will not, by itself, make the attachment privileged." *Leonen*, 135 F.R.D. at 98 (citing *Sneider v. Kimberly-Clarke Corp.*, 91 F.R.D. 1 (N.D. Ill. 1980)). The applicability of the attorney-client privilege is determined on a case-by-case basis, *Upjohn*, 449 U.S. at 396–97, and the burden of establishing that a document is protected by the attorney-client privilege is on the party asserting the privilege. *Torres v. Kuzniasz*, 936 F.Supp. 1201, 1208 (D.N.J. 1996).

The crime-fraud exception to the attorney-client privilege allows for disclosure of otherwise privileged communications when they are made with the intent to further a continuing or future crime or fraud. *Wachtel v. Guardian Life Ins. Co.*, 239 F.R.D. 376, 378 (D.N.J. 2006). The crime-fraud exception can encompass communications and attorney work product "in furtherance of an intentional tort that undermines the adversary system itself[,]" including the spoliation of evidence. *Id.* at 380 (internal quotation marks omitted). The purpose of the crime-fraud exception is "to assure that the seal of secrecy between lawyer and client does not extend to communications made for the purpose of getting advice for the commission of a fraud or crime." *Id.* at 378 (internal quotation marks omitted). The Third Circuit has established a multi-step process for determining whether a party's claim of privilege should be pierced by the crime-fraud exception. *Id.* First, the party seeking the discovery must make a prima facie showing that (1) the client claiming the privilege was engaging or intended to engage in a crime or fraud at the time of the attorney-client communication, and (2) that the communication was in furtherance of the continuing or intended crime or fraud. *Id.* (citing *In re Grand Jury Subpoena*, 223 F.3d 213 (3d Cir. 2000)). In order to satisfy the prima facie showing, the party opposing the privilege must demonstrate a "reasonable basis to suspect that the privilege holder was committing or intending to commit a crime or fraud and that the attorney-client communications or attorney work product were used in furtherance of the alleged crime or fraud[.]" *In re Grand Jury*, 705 F.3d 133, 153 (3d Cir. 2012). Under this standard, the party opposing the privilege is not required to present evidence sufficient to support a verdict of crime or fraud, or even to show that it is more likely than not that the crime or fraud occurred." *Id.* at 153-54. Rather, the prima facie showing requires evidence which "if believed by the fact-finder, would be sufficient to support a finding that the elements of the crime-fraud exception were met." *In re Grand Jury Subpoena*, 696 Fed.

Appx. 66, 70 (3d Cir. 2017) (internal quotation marks omitted). If the court determines that the party seeking discovery has presented sufficient evidence at stage one, then it may decide to conduct an *in camera* review of the contested documents. *Wachtel*, 239 F.R.D. at 379 (citing *United States v. Zolin*, 491 U.S. 554, 572 (1989)). The court then must determine whether the party asserting the privilege has sustained its burden of proof, specifically, whether it has given a reasonable explanation of its conduct. *Id.* Finally, the court must decide if it is more likely than not that the holder of the privilege sought or used legal advice to commit or try to commit a crime or fraud. *Id.* If the court accepts the explanation provided by the party asserting the privilege as sufficient to rebut the prima facie case made at stage one, the privilege will be upheld. *Id.* If the court finds the explanation insufficient to rebut the prima facie case, then the attorney-client privilege is pierced. *Id.*

III. Opinion

A. DataDestroyed Spreadsheet

The Special Master finds that the crime-fraud exception to the attorney-client privilege applies to the DataDestroyed Spreadsheet (Exhibits A-1 and A-2). Initially, the Special Master finds that the DataDestroyed Spreadsheet is a privileged document in that it was created at the direction of Veeva's in-house counsel, for the purpose of evaluating IQVIA's allegations in connection with this lawsuit. There is no dispute that the document was created post-litigation. Veeva has provided a certification from its in-house counsel, Josh Faddis, wherein he certifies that he instructed Veeva employee Rebecca Silver to create the spreadsheet to "catalog data collected from customers that received a DRC" so that Faddis could "evaluate IQVIA's lawsuit and assess any legal obligations Veeva had to customers and IQVIA regarding data obtained as

part of the DRC process." (Faddis Declaration at ¶¶ 20-21.) Furthermore, the document itself contains the following header "Privileged. Prepared at the direction of counsel[.]" (Exhibit A-1.)

Notwithstanding the foregoing, the Special Master finds that IQVIA has made a prima facie showing that Veeva was engaging or intended to engage in a crime or fraud at the time the DataDestroyed Spreadsheet was created and that the DataDestroyed Spreadsheet was used in furtherance of the alleged crime or fraud – namely, the spoliation of evidence. The Special Master has reviewed both versions of the DataDestroyed Spreadsheet and finds that they appear to track the deletion of evidence post-litigation. Although Faddis has certified that it was neither his intention nor his instruction that the DataDestroyed Spreadsheet be used for such a purpose, the document itself suggests that it was. The DataDestroyed Spreadsheet identifies documents and/or information in existence at the time of its creation, along with notations concerning whether those documents and/or information were deleted or needed to be deleted. For example, it contains a sheet which identifies certain documents and/or information that were "FOUND" at the time of its creation. (Exhibit A-2 at p. 3.) After identifying which documents and/or information were "FOUND," the sheet contains a column identifying "WHERE" that information was found, and then contains a column for "ACTION." (*Id.*) The "ACTION" column contains the following notations: "PURGED" or "ASK ERIC TO CHECK AND PURGE" or "ASK ZAK TO INVESTIGATE" or "ASK JEN AND ERIC TO LOOK." (*Id.*) As this document was created after litigation commenced, and it is identifying documents or information that were "FOUND" at that point in time, the fact that a column contains references to the documents being "PURGED" would suggest that these documents were deleted post-litigation. (*Id.*) Furthermore, the fact that the DataDestroyed Spreadsheet contains future-tense

language to "CHECK AND PURGE" documents or information that were found after litigation commenced, is further evidence that the spreadsheet tracks the deletion of evidence.

The foregoing is not the only reference to purging documents or information contained in the DataDestroyed Spreadsheet. Indeed, the spreadsheet contains another page referencing 2166 JIRA tickets that "should be viewed to check and see if the attachment should be purged[.]" (Exhibit A-2 at p. 4). Two other sheets in Exhibit A-2 contain similar directives. Exhibit A-2 also contains the following column titles: "Check," "Concern," "Action" and "Recommend." (*Id.* at pp. 6-7.) After identifying a variety of data/information, the "Action" column contains references to "Reviewed with team to remove old tables[.]" (*Id.*) The "Recommend" column contains references to "Remove" and "Remove old outputs." (*Id.*) The fact that this data/information was found at the time the spreadsheet was created, post-commencement of litigation, and identifies data/information that existed at the time, along with instructions or comments that such data/information should be removed supports the finding that this document tracked the deletion of evidence. Furthermore, the fact that Veeva provides no explanation for the future-tense language to purge or delete evidence in the document is telling.

Veeva alleges that IQVIA has failed to demonstrate that the missing evidence is relevant. The Special Master disagrees. Veeva's in-house counsel certifies that the DataDestroyed Spreadsheet was created in direct response to IQVIA's lawsuit. Specifically, he states that "[t]he point of the spreadsheet was to track and catalog data collected from customers that received a DRC, so that I could evaluate IQVIA's lawsuit and assess any legal obligations Veeva had to customers and IQVIA regarding data obtained as part of the DRC process." (Faddis Declaration at ¶ 22.) He also states that the spreadsheet was "intended and designed to inform my legal analysis regarding Veeva's DRC practices[.]" (*Id.* at ¶ 22.) Veeva also acknowledges that

IQVIA's lawsuit specifically asserted claims concerning Veeva's use of DRCs to steal IQVIA's proprietary information. (*Id.* at ¶ 21.) Thus, it is hard to reconcile how certain information was deemed relevant to Veeva in its evaluation of its legal obligations in connection with this lawsuit, yet irrelevant for preservation purposes.

Moreover, Veeva's contention that because it produced some extracts identified in the DataDestroyed Spreadsheet, it could not have schemed to delete other customer extracts is belied by the discovery produced in this matter. Veeva's interrogatory responses identify nineteen extracts in the DataDestroyed Spreadsheet that were deleted and not produced in discovery, and another eight that are identified in the DataDestroyed Spreadsheet that were not even identified in Veeva's interrogatory responses. The production of some data extracts in discovery does not forgive the deletion of others.

Thus, for the foregoing reasons, the Special Master finds that IQVIA has made a prima facie showing that Veeva was engaging or intended to engage in a crime or fraud – specifically the spoliation of evidence – and that the DataDestroyed Spreadsheet was used in furtherance of that purpose. The Special Master has conducted an *in camera* review of the document and is unsatisfied by Veeva's explanation to rebut the prima facie case. Accordingly, the Special Master finds that the DataDestroyed Spreadsheet is discoverable pursuant to the crime-fraud exception to the attorney-client privilege.

B. Cover-Up Documents

IQVIA argues that the Cover-Up Documents are not privileged because they were created for a business purpose, not to provide legal advice or for the purpose of litigation. IQVIA further argues that even if they did contain legal advice, they are subject to the crime-fraud exception. Veeva argues that these documents are privileged because they were sent to Veeva's in-house

counsel for his legal review. The Special Master finds that the Cover-Up Documents are not subject to the attorney-client privilege because they were created for a business purpose and do not contain any requests for or provision of legal advice.

It is undisputed that the OpenData Data Corruption Memo was prepared by non-lawyer Veeva executives at the request of Veeva's CEO. Specifically, on September 25, 2015, Veeva's CEO, Peter Gassner, requested a written plan "that goes to me from Brian [Longo] with copy to Tim [Slevin] and Rebecca [Silver]." (IQVIA Exhibit EE.) Although Veeva's in-house counsel, Josh Faddis, is copied on the e-mail, there is no request for legal advice. (*Id.*) In response, Longo wrote a memorandum "assessing the scope of the Genentech data issues and proposing responses." (*See* Declaration of Brian Longo in Opposition to the Privilege Motion ("Longo Declaration") at ¶ 5.) Longo certifies that he "led the Veeva team analyzing the Genentech data issues and proposed next steps to Veeva's senior leadership, including General Counsel Josh Faddis and CEO Peter Gassner." (*Id.* at ¶ 4.) As part of that effort, Longo and other Veeva employees "wrote a memorandum assessing the scope of the Genentech data issues and proposing responses." (*Id.* at ¶ 5.) Longo further certifies that the memo was "edited over several days in late-September 2015, to reflect new analysis and insights regarding the scope of the Genentech data issues." (*Id.*) Longo states generally that when he was preparing the memorandum he "knew that Mr. Faddis would review the document to determine whether Veeva had any legal obligations arising from the discovery of the Genentech data issues" and that he "sent the Genentech memorandum to Mr. Faddis for his legal review." (*Id.* at ¶¶ 7-8.) Longo "believed Mr. Faddis's legal advice was a necessary consideration for any corporate response." (*Id.* at ¶ 8.) Longo also certifies that Faddis did in fact provide legal advice and that he and

Faddis "discussed the memorandum, the underlying analysis, and the relevant issues." (*Id.* at ¶ 9.)

Although Longo states that he ultimately sent the OpenData Data Corruption Memo to Veeva's in-house counsel, Veeva does not indicate which version of the document was sent to in-house counsel, and does not provide any contemporaneous evidence demonstrating that legal advice was provided by in-house counsel with respect to the document. Indeed, on September 26, 2015, Faddis wrote to Longo that he had not yet reviewed the memo and that Veeva's CEO was aware and "not thinking [Faddis is] working on this." (IQVIA Exhibit DD.) It appears this was in response to Version 3 of the memo, although it is unclear from the motion papers how many versions of the memo exist. Veeva contends that the memorandum explicitly calls for Faddis's legal analysis and cites to pages 9-10 of Exhibit A-3. The Special Master has reviewed these pages, and both versions of the document in full (Exhibits A-3 and A-4), and finds that neither draft contains legal advice on its face. The OpenData Data Corruption Memo identifies a task that was assigned to Faddis, but notes that it is not yet started.

Faddis provides a certification in which he states, generally, that he provided legal advice regarding the "Genentech [I]ncident[,]" specifically with respect to: "Veeva's obligations under TPAs"; "Veeva's assessment and potential responses to the inadvertent access to IQVIA address records" and "Veeva's legal exposure to IQVIA and Genentech[.]" (*See* Faddis Declaration at ¶ 12.) Faddis further states that the "Genentech memorandum and the underlying analysis" were "prepared, in part, to help [him] assess whether Veeva faced any legal risk and determine whether Veeva had any legal obligations to Genentech and others." (*Id.* at ¶ 14 (emphasis added).) He also states that his legal advice was "requested and necessary before senior management could offer a recommendation to [Veeva's CEO]" and that while he did not author

the memorandum, he reviewed it and provided legal advice, "which informed Veeva's decision-making process." (*Id.* at ¶ 15.) Despite this certification, Veeva has not produced any evidence that Faddis provided legal advice with respect to the OpenData Data Corruption Memo or any of its versions.

The evidence produced suggests the document was created for a primarily business purpose – namely, formulating a business response to the Genentech Incident. Veeva has failed to produce any evidence indicating when Faddis reviewed the document, which version of the document he reviewed, or the alleged legal advice that he rendered with respect to the document. Veeva contends that "contemporaneous evidence" demonstrates that Faddis provided legal advice with respect to these documents because he assigned "To-Dos" to Veeva employees as the Genentech investigation was underway. (Veeva Opp. Br. at p. 13.) Notably, the exhibit that Veeva cites to support this argument is Exhibit A-34. Exhibit A-34 contains an e-mail chain dated September 21, 2015, in which Longo sets forth To Dos "as instructed by Josh[.]" This e-mail chain pre-dates Veeva CEO Peter Gassner's request for creation of the memo. Thus, it does not demonstrate that Faddis provided legal advice in connection with the OpenData Data Corruption Memo. Faddis's general references to reviewing the document and subsequently providing legal advice are insufficient to satisfy Veeva's burden of establishing that this document is predominantly legal in nature and protected by the attorney-client privilege.

Veeva also contends that there is contemporaneous evidence demonstrating that Longo sought out Faddis's advice in drafting the OpenData Data Corruption Memo. (Veeva Exhibits A-5, A-44, and A-47.) However, Exhibits A-44 and A-47 contain portions of the same e-mail chain, and the same request to in-house counsel for comment on the draft memorandum. They are not separate requests for legal advice. Nor is it clear from the e-mails provided whether the advice

sought from Faddis was legal or business in nature, or that Faddis actually provided legal advice with respect to the memorandum, as opposed to the Genentech Incident in general. Veeva also argues that *In re Ford Motor Co.*, 110 F.3d 954 (3d Cir. 1997) is controlling here and protects business communications between executives and in-house counsel that were made for the purpose of securing legal advice. (Veeva Opp. Br. at pp. 15-16). The Special Master finds *In re Ford Motor Co.* to be distinguishable. In that case, the first set of documents sought contained minutes of a meeting of top Ford executives, including general counsel, during which, the general counsel briefed the committee about a report he had drafted concerning the subject vehicle. *Id.* at 957. The court reviewed the documents *in camera* and determined that they reflected Ford's concern about the subject vehicle in its early stages of development and counsel's examination of the legal implications of some of those concerns and recommended course of action. *Id.* at 966. The second set of documents sought contained a series of agendas, with handwritten notes, concerning litigation defense strategy in connection with a variety of lawsuits that had been filed with respect to the subject vehicle. *Id.* at 957. The court also reviewed these records *in camera* and concluded that they disclosed legal strategy for defending lawsuits such as the one at issue in that particular case. *Id.* at 967. For the reasons set forth in this opinion, that is not the case for these documents.

Veeva likens its claims of privilege with those asserted by IQVIA in a prior discovery motion in this matter. The Special Master will note only that the documents submitted by IQVIA for *in camera* review were draft versions of PowerPoint presentations that explicitly contained legal advice, something noticeably absent from the documents submitted by Veeva for *in camera* review. Furthermore, IQVIA produced the final versions of the PowerPoints in discovery. Thus, ordering production of the various drafts of the PowerPoints would inevitably disclose the legal

advice sought and rendered. Here, the Cover-Up Documents do not contain legal advice, nor would their production allow IQVIA to determine the context of legal advice sought or rendered.

At the very least, the OpenData Data Corruption Memo has a mixed business and legal purpose and in order to apply the attorney-client privilege to this document, Veeva must demonstrate that the primary purpose of the communication was to aid in the provision of legal advice. Veeva fails to satisfy this burden. Furthermore, the e-mail chain forwarding the draft of the OpenData Data Corruption Memo (Exhibit A-5) merely copies in-house counsel. It does not request legal advice nor does it contain legal advice. Merely copying an attorney on an e-mail does not, in and of itself, make the e-mail privileged. *In re Human Tissue Products Liability Litigation*, 255 F.R.D. at 164. Thus, the Special Master finds that the Cover-Up Documents are not privileged and subject to disclosure. Having so concluded, the Special Master does not reach IQVIA's argument concerning whether the crime-fraud exception applies to the Cover-Up Documents.

C. Other Privileged Documents

The Special Master has conducted an *in camera* review of the fifty-four Other Privilege Documents, which Veeva categorizes as follows: (1) Documents Containing Legal Advice Regarding TPA Agreements (Exhibits A-8 through A-19); (2) Documents Containing Legal Advice Regarding the E&Y Audit (Exhibits A-20 through A-31); (3) Documents Containing Legal Advice Relating to Genentech Incident (Exhibits A-32 through A-56); and (4) Documents Containing Conversations Among Non-Lawyer Employees (Exhibits A-57 through A-61). The Special Master will address each category in turn:

1. *Documents Containing Legal Advice Regarding TPA Agreements (Exhibits A-8 through A-19)*

The Special Master has reviewed these documents and concludes that Exhibits A-8 through A-19 are privileged as set forth by Veeva. They contain requests for legal advice, actual legal advice, discussion of legal advice, or requests for information in connection with legal advice concerning Veeva's TPA agreements. In most instances, in-house counsel is the target recipient of these e-mails and/or directly responded to the e-mails with legal advice. Specifically, Exhibits A-10, A-11, A-16, A-18 and A-19 are privileged in full. The remaining exhibits are privileged in part, as set forth by Veeva in the documents produced for *in camera* review.

2. *Documents Containing Legal Advice Regarding the E&Y Audit (Exhibits A-20 through A-31)*

Veeva argues that Exhibits A-20 through A-31 are privileged because Veeva's in-house counsel "negotiated the terms of the audit, provided legal advice regarding Veeva's preparation for and participation in the audit, and asked employees to assemble materials for legal review." (Veeva Opp. Br. at p. 22.) Veeva further contends that these documents contain requests for legal advice from Veeva employees to Veeva's in-house counsel. Veeva also contends that it undertook an internal investigation to assess its compliance with contractual and other data-handling requirements, in which Veeva's in-house counsel participated. IQVIA argues that in responding to the E&Y Audit, Veeva engaged in fraud on the Court by spoliating evidence and attempted fraud on IQVIA by lying to auditors, and asks the Special Master to review the documents *in camera* and order production of any which are not privileged or were used in furtherance of the above-referenced frauds.

The Special Master has conducted an *in camera* review of these documents. With respect to Exhibits A-20, A-21, A-22, and A-30, the Special Master concludes that Veeva has not

satisfied its burden of establishing that the documents are protected by the attorney-client privilege. Exhibit A-20 copies Veeva's in-house counsel, who asks whether there are any tasks specifically assigned to her. Another Veeva employee responds that there are not, and includes his thoughts on what the auditors might look at in connection with the E&Y Audit. There is no request for nor any legal advice provided in this e-mail. Exhibit A-21 is the same e-mail chain as Exhibit A-20, with a response from Veeva's in-house counsel, thanking the Veeva employee for the update. This document does not contain any requests for nor provision of legal advice and is thus, not privileged. Exhibit A-22 is an e-mail chain that contains a discussion between Veeva's in-house counsel and IQVIA's in-house counsel, which is then forwarded by Veeva's in-house counsel to another Veeva employee to advise him of the status of the request. There is no request for legal advice and no provision of legal advice. Rather, Veeva's in-house counsel comments on his understanding of the status of those discussions, which does not contain the provision of any legal advice. Exhibit A-30 is an e-mail chain between Veeva employees. The hard copy produced to the Special Master for *in camera* review indicates that it is an e-mail chain, but it does not show which parties were copied on each response in the e-mail chain. Thus, it is difficult to ascertain at what point in-house counsel may have been added to the conversation. It appears, from the face of the document, that in-house counsel was not included in the discussion until the final e-mail in the chain, which does not contain any requests for nor provision of legal advice. Furthermore, a portion of this exact e-mail chain is a part of Exhibit A-28, and was not identified as privileged by Veeva in that exhibit. Specifically, the first e-mail in the chain (sent by David Tsao, dated October 12, 2015, at 8:57 P.M.) through the October 13, 2015, 3:59 P.M. e-mail from David Tsao, is also contained in Exhibit A-28 and is not identified as privileged by Veeva (with the exception of one sentence in the October 13, 2015, 3:59 P.M. e-mail from David

Tsao). The remainder of the e-mail chain in Exhibit A-30 contains a discussion between Veeva employees. There is no indication that the discussion requests legal advice, is provided in response to a request from Veeva's in-house counsel for information, or otherwise renders legal advice. Thus, the Special Master finds that Veeva has not satisfied its burden of establishing that this particular e-mail chain is protected by the attorney-client privilege.[9]

However, with respect to Exhibits A-23 through A-29, and A-31, the Special Master finds they are privileged in part, and orders production of the documents with redactions as set forth by Veeva in the hard copy produced to the Special Master for *in camera* review. With respect to Exhibit A-29, it is an e-mail chain. The first message in the chain is an e-mail from David Tsao, dated October 12, 2015, to Josh Faddis, Brian Longo, Jacques Mourrain, and Stan Wong. This particular e-mail appears in Exhibit A-28 and was not identified by Veeva as a privileged communication in that exhibit. The Special Master finds that Veeva has not satisfied its burden of demonstrating that this particular e-mail chain is subject to the attorney-client privilege because it does not contain any requests for nor provision of legal advice and there is no evidence that it was prepared at the direction of counsel or in furtherance of counsel's efforts to provide legal advice. Thus, the Special Master finds that Exhibit A-29 should be produced with the initial e-mail from David Tsao, dated October 12, 2015, at 5:58 P.M. unredacted, but the remainder of the document may be redacted as it reflects legal advice sought and provided and is protected by the attorney-client privilege. Likewise, a substantial portion of the e-mail chain in Exhibit A-31 appears in Exhibit A-28 and is not redacted there. For the reasons set forth above, and consistent with the Special Master's ruling, Veeva is to produce Exhibit A-31, but may redact the October 13, 2015, 4:25 P.M. e-mail from Josh Faddis, and the October 14, 2015, 5:00

[9] Veeva may redact the one sentence in the October 13, 2015, e-mail from David Tsao that is also highlighted in Exhibit A-28.

A.M. response from Brian Longo, which the Special Master finds are protected by the attorney-client privilege. Furthermore, the Special Master also finds that the attachment to the e-mail chain in Exhibit A-31 is privileged as it contains counsel's legal advice.

3. *Documents Containing Legal Advice Relating to the Genentech Incident (Exhibits A-32 through A-56)*

The Special Master has reviewed these documents and concludes that Exhibits A-33, A-35, and A-36 are privileged in full and protected from disclosure. Exhibits A-39 through A-42, A-46, and A-49 through A-55 are not privileged and subject to disclosure. Exhibit A-32 contains a cover e-mail, which the Special Master finds to be protected by the attorney-client privilege; however, the attached document is not privileged. Exhibit A-34 contains a cover e-mail, which the Special Master finds to be privileged in part, as set forth by Veeva. However, the attachment is not privileged. Exhibit A-56 contains the same e-mail chain as Exhibit A-34, which the Special Master finds to be privileged in part, as set forth by Veeva. Exhibits A-44, A-45, A-47, and A-48 contain the same e-mail chain, which the Special Master finds to be privileged in part, and shall be produced with the redactions set forth by Veeva. However, the attachments contained in Exhibits A-44, A-47, and A-48 are not privileged and shall be produced. Exhibit A-43 appears to be a draft of the OpenData Data Corruption Memo. The Special Master notes that Veeva offers no independent explanation for why this document is privileged, when or by whom it was prepared, or to whom it was sent. The Special Master has reviewed this document, however, and concludes that it is privileged in part. Specifically, the final paragraph of the document, beginning with the number "5" shall be redacted. Finally, the Special Master finds that Exhibits A-37 and A-38 are privileged in part. The cover e-mails are privileged as set forth by Veeva. However, the attachments to these exhibits are not privileged.

4. *Documents Containing Conversations Among Non-Lawyer Employees (Exhibits A-57 through A-61)*

The Special Master has conducted an *in camera* review of these documents. Exhibit A-57 is a conversation between Veeva employees Vincent Pavan and Angelique Aldaya. Neither is an attorney. The Special Master notes that Veeva has the burden of demonstrating that the document is privileged and that burden applies to each document for which Veeva asserts the privilege. Veeva's argument with respect to Exhibit A-57 is one sentence long and contains a generalized statement that the exhibit "includes a discussion of information conveyed to in-house counsel for the purpose of assisting counsel to provide legal advice, and thus is privileged under settled law." (Veeva Opp. Br. at p. 25 (citing *Symetra Life Ins. Co. v. JJK 2016 Ins. Tr.*, 2019 WL 4931231, at *5 (D.N.J. Oct. 7, 2019) ("In the case of a corporate client, privileged communications may be shared by non-attorney employees in order to relay information requested by attorneys."))). There are two statements that Veeva highlights within this document, wherein Pavan allegedly repeats information that he provided to or received from Veeva's in-house counsel. Veeva does not provide any context for the Special Master, nor any factual background to demonstrate that the purportedly highlighted portion reflects legal advice sought or received. Although the Special Master could conclude that Veeva has failed to satisfy its burden that the highlighted portion of the document is privileged, based on the Special Master's extensive review of the Other Privileged Documents, it appears as if the highlighted portion of Exhibit A-57 does reflect legal advice. However, the remainder of the exhibit is not privileged. Thus, Veeva may redact the highlighted statements from the conversation, which should otherwise be produced.

The Special Master finds that Exhibits A-58, A-59, and A-60 are conversations between Veeva employees Silver and Slevin (Exhibit A-58), and Kahan (Exhibits A-59 and A-60), which

are not protected by the attorney-client privilege. Veeva argues that these exhibits are privileged because they were "made during an investigation regarding legal compliance" and the privilege extends to "statements made by employees assisting counsel, seeking information to provide to counsel so that counsel can provide legal services." Veeva relies upon a certification from Silver, wherein she states that Exhibits A-58, A-59, and A-60 contain communications that she made as "part of [her] efforts to collect information for Mr. Faddis and others to review in preparation for the audit." (*See* Declaration of Rebecca Silver in Opposition to the Privilege Motion at ¶ 5). The Special Master finds that these communications are not privileged. They are conversations between non-lawyers that do not contain any request for legal advice, do not reference any privileged communications, do not reference counsel or mention any request from counsel to obtain certain information, and there is no contemporaneous evidence suggesting that counsel did in fact request that this information be sought out and obtained by Ms. Silver. The Special Master finds that the predominant purpose of these documents was to address business concerns, not legal concerns. Thus, they are not privileged and are discoverable.

Exhibit A-61 is an e-mail from Veeva employee Tim Slevin to Veeva employee Brian Longo with an attachment. Veeva argues that Exhibit A-61 is privileged because Slevin "made the protected communication to Longo so that Longo would present his views to Veeva's senior management at the September 2019 OPS meeting." However, the face of the e-mail is not consistent with this representation. Rather, the e-mail indicates that Slevin is sending a document to Longo for Longo's review and input. It contains no request for legal advice, neither party to the e-mail is an attorney, nor does it request that Longo present the document to in-house counsel for legal advice. There is no contemporaneous evidence submitted by Veeva to support its

contention that this document was created for the purpose of obtaining legal advice. Therefore, the Special Master finds that A-61 is not privileged.

D. Slevin E-mail

The Special Master concludes that the Slevin E-mail is not subject to the attorney-client privilege. The Slevin E-mail was prepared by Veeva employee Tim Slevin. It is a September 25, 2015, e-mail to his wife, Susan Slevin, which contains a draft e-mail that he prepared to Veeva CEO, Peter Gassner, concerning the Genentech Incident. Susan Slevin responds to the e-mail with her feedback. No attorney is copied on the e-mail. It is a communication between spouses. Veeva contends that a portion of the Slevin E-mail is privileged because Mr. Slevin includes a statement that in-house counsel's input is needed with respect to his recommendations contained in one paragraph in the e-mail. The Special Master is not persuaded by this argument. There is no explicit request for legal advice in the document, nor was the document prepared for or sent to legal counsel. Thus, the Special Master concludes that the Slevin E-mail is not privileged and subject to disclosure.

E. Procedural Propriety of Motion

Veeva argues that IQVIA's motion should be denied because it is procedurally improper. Specifically, Veeva argues that IQVIA failed to engage in a meet and confer, and that its challenges to the clawed back documents are untimely under the DCO, which requires such challenges to be made within a "reasonable time." IQVIA counters that it made multiple attempts to obtain further information about Veeva's privilege assertions, to no avail. IQVIA also contends that its delay (between 30-90 days) is reasonable given the winter holiday and the extensive discovery in which the parties were engaged at the time. The Special Master finds that IQVIA asserted its challenges to Veeva's clawed back documents within a reasonable period of

time as contemplated by the DCO. The Special Master also finds that while a greater effort to meet and confer could have been made, the communications between counsel generally satisfied Rule 37(a)(1)'s requirement, and that further discussions between the parties were unlikely to have resolved the issues raised by this motion.

Sanctions Motion

I. Introduction

IQVIA requests sanctions against Veeva for Veeva's alleged spoliation of highly probative evidence. IQVIA argues that Veeva intentionally and permanently deleted evidence that is central to IQVIA's case; did so, in some cases, after the Special Master ordered Veeva to produce the evidence in question; and lied about its misconduct to avoid detection by IQVIA and the Court. Specifically, IQVIA contends that Veeva should have anticipated litigation in September 2015, and thus, any evidence destroyed in connection with the Genentech Incident and the Shire Incident constitutes spoliation of evidence. IQVIA also contends that Veeva deleted evidence after it filed this lawsuit – namely, EUStage, documents contained in Google Drive, and various James Kahan e-mails. IQVIA contends that Veeva acted with the highest level of intent and therefore, seeks case-terminating sanctions. Alternatively, IQVIA requests an adverse inference charge.

II. Arguments of the Parties

A. Genentech Incident

1. IQVIA's Arguments

IQVIA contends that Veeva deleted evidence in September 2015 upon learning of the Genentech Incident and in advance of the E&Y Audit. The E&Y Audit was originally scheduled for September 28, 2015. On September 10, 2015, Veeva was sent a Pre-Audit Questionnaire

prepared by the auditor, which asked Veeva to provide a "complete list" of IQVIA data in Veeva's possession. Veeva engaged in an internal investigation, during which it learned of the Genentech Incident set forth above. IQVIA contends that during the internal investigation, Veeva uncovered two dozen folders containing "IMS Data," which Veeva was not authorized to possess. Veeva also learned that the IQVIA data was being programmatically included in Veeva OpenData and was visible to OpenData stewards who were responsible for improving and maintaining OpenData. IQVIA further contends that it will never know exactly what these files contained because Veeva subsequently deleted them. IQVIA points to certain statements made by Veeva employees Silver (Veeva's Vice President of OpenData North America) and Longo (Veeva's General Manager of Commercial Products) to demonstrate that Veeva anticipated litigation at that time. For example, in regards to the Genentech Incident, Silver remarked to one of her colleagues – "The further I dig the scarier it gets." Likewise, Longo expressed: "If I were [IQVIA], I would hang us with this info."

Upon learning about the Genentech Incident, Veeva CEO Gassner asked Silver, Longo, and Slevin to prepare a written plan documenting their findings and recommending next steps. In conjunction, the three authored the OpenData Data Corruption Memo, which IQVIA contends demonstrates that Veeva immediately understood the import of its findings and anticipated that litigation with IQVIA would ensue. For example, the OpenData Data Corruption Memo stated that the E&Y Audit "has a high likelihood of exposing the data corruption issue." IQVIA further contends that Veeva anticipated litigation in September 2015 because during this lawsuit, Veeva has asserted work-product privilege on the basis of "anticipation of litigation" over numerous documents created from September 25, 2015, onward.

IQVIA argues that ultimately, Veeva chose not to disclose any information concerning

the Genentech Incident to IQVIA or the auditors. Instead, Veeva twice delayed the E&Y Audit under the pretense that the agreements relating to the audit required further review, and used that time to construct its cover up. In particular, IQVIA contends that Veeva wiped files saved in over two hundred directories on its NAS server, including the IMS data files discussed above, which Veeva knew it had no right to possess. Veeva personnel also tracked down other IQVIA data in their possession in order to delete evidence of their access to that data as well. Veeva also deleted thousands of tables within its HDM database that showed that Veeva had misappropriated IQVIA data. This included Veeva's deletion of hundreds of data tables related to Veeva's programmatic inclusion of IQVIA data in OpenData. Veeva also deleted over 1,100 Data Validation Interface ("DVI") tables that documented how Veeva had built Veeva OpenData over the years through data stewardship. IQVIA contends that although the tables no longer exist, the names of the destroyed tables indicate that many included IQVIA's proprietary data. IQVIA also contends that Veeva took steps to obstruct future discovery by sanitizing e-mail records, including instructing employees to "stop e-mailing" about Veeva's misappropriation of IQVIA data, substituting "***" for "IMS" in e-mails, and avoid using "key words" in e-mails concerning the Genentech Incident.

2. Veeva's Arguments

Veeva contends that it had no reason to anticipate litigation in connection with the Genentech Incident because it was minor and swiftly rectified. Veeva argues that in the fall of 2015, it agreed to the E&Y Audit of its data security controls of Veeva Network. In preparation for the audit, Veeva conducted a comprehensive internal investigation, during which it discovered unrelated access configuration errors in a different (i.e., non-Network) database used by Veeva for customer-specific professional services projects. Those errors, which originated from a

company Veeva had acquired years earlier, allowed IQVIA records provided to Veeva by customer Genentech to be included as a contributing source in Veeva's address-validation process. Further, the database storing those records was viewable by Veeva's OpenData data stewards. Veeva further argues that certain Veeva employees mobilized to investigate, uncertain about the extent of the problem, which it concludes was an overblown reaction. Further examination revealed that any "corruption" caused by the configuration errors was minor, isolated, and fixable. There was no evidence that a data steward ever had accessed the impacted database to update OpenData. Veeva contends that the configuration errors resulted in only 1,350 address records being included as a contributing source in Veeva's address validation process, out of more than 10 million OpenData records. Veeva further contends that it had independently collected each of the 1,350 addresses from independent, non-IQVIA sources. Veeva also argues that its non-disclosure of the Genentech Incident had no affect on the E&Y Audit because the investigation was outside of the scope of the audit – which only pertained to Veeva Network. Veeva contends that the Pre-Audit Questionnaire defining the audit's parameters asked whether Veeva obtained IQVIA data "with the intention or expectation [that] the data may be used in Veeva Network[,]" to which it accurately responded "no." The Genentech Incident involved a professional services project and the database used for that project, not Veeva Network. Veeva did not intend or expect to, and in fact never did, use Genentech's IQVIA data in Veeva Network.

Veeva contends that at the time of the Genentech Incident, it believed it could resolve the TPA issues with IQVIA through negotiations, assurances, and audits, and had no reason to anticipate that it would lead to litigation. IQVIA points to the OpenData Data Corruption Memo, which was prepared by Veeva executives in response to the Genentech Incident, as support for

its argument that Veeva should have anticipated litigation at that time. Veeva counters that its contemporaneous investigation into that issue disproves that Veeva anticipated, or should have anticipated, litigation upon discovering the supposed "corruption." Veeva contends that its investigation revealed that the Genentech Incident (1) arose before Veeva acquired the database at issue; (2) affected only 0.00063% of the Veeva OpenData address dataset; and (3) other sources such as State Medical Boards and the Drug Enforcement Administration supplied the same address records. Veeva also contends that IQVIA's reaction to the Shire Incident further confirms that it had no reason to anticipate litigation before the lawsuit was actually filed. Rather than threaten litigation in connection with the Shire Incident, IQVIA thanked Veeva for its prompt response and handling of the situation – which included deleting IQVIA records from its database. Veeva further argues that certain statements made by Veeva non-executives, expressing concern over the potential for litigation are non-binding, were speculative, and did not activate a duty to preserve.

3. IQVIA's Reply

In reply, IQVIA contends that Veeva's defense that it did not anticipate litigation in September 2015 is belied by the facts. Specifically, IQVIA argues that if Veeva really thought that IQVIA would agree that Veeva's trade-secret theft "was minor, isolated, and fixable," then Veeva would have come clean about its theft. It would not have delayed the audit under false pretenses so it could destroy evidence of its guilt. Furthermore, IQVIA argues that commentary from Veeva executives concerning the severity of the Genentech Incident was not simply "rumor and watercooler gossip," rather, the statements were expressions of concern made by Veeva executives responsible for Veeva's internal investigation. IQVIA also argues that Veeva's in-house counsel's claim that he did not personally anticipate litigation in connection with the

Genentech Incident should be disregarded because the standard is an objective, not a subjective, one. IQVIA contends that Veeva's previous assertions of work-product privilege over documents created in September 2015 demonstrate that Veeva anticipated litigation as of that time, and Veeva did not withdraw those claims until after Veeva became aware that IQVIA's spoliation motion was forthcoming. IQVIA contends that Veeva's claim that it was blindsided by IQVIA's lawsuit is disingenuous given that Veeva was hiding its misappropriation. Furthermore, IQVIA argues that Veeva's claim that the Genentech Incident was outside of the scope of the E&Y Audit is false because the audit specifically asked about OpenData and the theft was identified in Veeva's HDM database – which was used to build OpenData.

IQVIA further contends that Veeva's deletion of evidence of its theft in HDM is sanctionable spoliation. IQVIA argues that the deleted evidence is relevant and that Veeva intends to use the absence of such evidence to argue that IQVIA cannot prove its case. For example, the deleted evidence includes: over 200 directories in Veeva's NAS server within HDM including dozens of IQVIA's Reference Data files, as well as thousands of client history, DVI, and Projects tables and databases from HDM. IQVIA contends that Veeva's argument that the Genentech Incident involved only 1,350 address records affecting only 0.00063% of OpenData address dataset is misleading. IQVIA notes that even taking this representation at face value, it only pertains to the direct contribution of IQVIA Reference Data to OpenData via Genentech. However, Veeva was aware of nine other customers with a similar issue, but was unable to confirm whether such customers had IQVIA Reference Data. Indeed, IQVIA argues, Veeva specifically instructed employees not to look for new customer issues and focus only on Genentech data. IQVIA contends that Veeva's destruction of evidence from HDM has made it impossible for IQVIA to reconstruct and determine the exact extent of the theft. Furthermore,

IQVIA notes that its Reference Data was visible to Veeva OpenData data stewards and it is unclear whether and to what extent they may have used that information to improve Veeva OpenData. Thus, Veeva is using the absence of such evidence as both a sword and a shield.

IQVIA also disputes that Veeva's deletions occurred in the ordinary course because they were not done by any automated system, but rather, they were done through the affirmative actions of Veeva employees and at the direction of Veeva executives. For example, IQVIA notes that Veeva deleted all 200 NAS directories from HDM on the same day, October 13, 2015, which was less than two weeks before the E&Y Audit was set to begin. Veeva also deleted the client history, DVI, and Projects tables during the time of the audit, at or around October 29, 2015. IQVIA argues that Veeva fails to identify any standard operating procedures ("SOPs") in place during the fall of 2015 to justify such deletions. IQVIA also argues that Veeva's argument that it deleted the data in accordance with TPA agreements is disingenuous because, in many instances, there were no TPA agreements in place that authorized Veeva's access to the IQVIA Reference Data. IQVIA further argues that the HDM data is irrevocably lost and that Veeva cannot show that there is any overlap between the subset of data produced and that destroyed to suggest that IQVIA has not been prejudiced.

4. Veeva's Sur-Reply

Veeva contends that it had a SOP to delete customer data after a project's completion. To support this contention, Veeva points to a statement by a Veeva employee in a JIRA ticket that certain data "need[s] to be purged per our 30 day SOP." Veeva also relies upon testimony from Veeva manager Brian Uber that the deletions which IQVIA contends are spoliation amounted to "cleanup of old project files" pursuant to Veeva's "cleanup SOP." Veeva further contends that the deletion of multiple customer files on the same day does not demonstrate ill-will, but rather

shows that Veeva found certain data extracts, which should have been deleted pursuant to the 30-day SOP, and proceeded to delete them in good faith to comply with customer obligations.

5. IQVIA's Response to Veeva's Sur-Reply

IQVIA argues that Veeva's claim, that IQVIA's response to the Shire Incident confirms that the similar Genentech Incident did not create a likelihood of litigation, is illogical and chronologically inconsistent. Specifically, the Shire Incident occurred in May 2016, eight months after the Genentech Incident. Thus, IQVIA argues, it could not possibly have affected whether Veeva should have anticipated litigation in connection with the Genentech Incident. IQVIA also argues that Veeva's internal documents indicate that it anticipated litigation in connection with the Shire Incident as well as the Genentech Incident. IQVIA contends that Veeva's "great data purge" of incriminating evidence following the Shire Incident further demonstrates that it anticipated litigation at that time. Furthermore, IQVIA argues that it did not amicably resolve the Shire Incident with Veeva because it ultimately sued Veeva for damages arising from the Shire Incident. IQVIA further argues that Veeva's alleged SOP requiring deletion of certain data is false. IQVIA contends that the very SOP on which Veeva relies was created after the October 2015 deletions.

B. Shire Incident

1. IQVIA's Arguments

IQVIA argues that Veeva deleted evidence in May 2016 in connection with the Shire Incident. IQVIA contends that Veeva would ask clients to send it data that Veeva knew IQVIA considered to be proprietary under the pretense that Veeva would run a DRC or DIR on the data. Veeva would then extract IQVIA's data and match it against Veeva's reference data, summarize the results, and forward the summary to sales people for use in a marketing presentation. IQVIA

further contends that after Veeva anticipated litigation with IQVIA, it proceeded to delete virtually every piece of evidence that would allow IQVIA to prove how Veeva used the IQVIA data to improve OpenData. Veeva engaged in various "purges" and "clean-ups," but some evidence slipped through the cracks. In May 2016, mutual client Shire expressed concern after a Veeva OpenData sales person asked Shire IT for permission to conduct a DIR, which was granted, and then withdrawn once Shire realized it did not have authority to grant such access. IQVIA argues that anticipating litigation with IQVIA, Veeva instructed employees to delete instant messages, e-mails, and other documents concerning the Shire Incident. Indeed, IQVIA points to various internal communications among Veeva employees referencing the "purge" and the "great data purge."

2. Veeva's Arguments

Veeva argues that the Shire Incident did not give rise to an anticipation of litigation with IQVIA because Shire misrepresented to Veeva that it had permission to share IQVIA Reference Data with Veeva, and that when Veeva learned that was not the case, it promptly rectified the situation by deleting the IQVIA Reference Data. Veeva contends that after Shire informed IQVIA about the incident, Veeva assured IQVIA that it had deleted the Reference Data and that "no extracted data was contributed to Veeva OpenData, Veeva data stewards or the system that maintains Veeva OpenData." Veeva also provided IQVIA with a certificate documenting Veeva's deletion of the customer extract from its system. Veeva further contends that in response to its efforts – which included deleting IQVIA data from its system – IQVIA thanked Veeva for its prompt resolution of the problem and did not threaten litigation or request that Veeva preserve the customer extract. Veeva argues that IQVIA's reaction to the Shire Incident, which it classifies as substantially similar to the Genentech Incident, shows that it had no reason to

anticipate litigation for either incident.

Veeva argues that IQVIA also takes issue with the deletion of certain instant message conversations and other materials in connection with the Shire Incident, but that any deletions involved ordinary-course document retention issues unrelated to the anticipation of litigation and that none of the deletions carries any legal significance. Veeva also argues that the customer data at issue is irrelevant to IQVIA's trade secret claims and that much of the purportedly deleted materials were recovered and produced in discovery.

3. IQVIA's Reply

IQVIA maintains that Veeva should have anticipated litigation in connection with the Shire Incident because Veeva employees expressed concern over the severity of the incident. Furthermore, IQVIA argues that Veeva's argument that IQVIA thanked Veeva for its prompt response in handling the Shire Incident is disingenuous given that in the same correspondence, IQVIA noted that the Shire Incident was an example of the concerns that IQVIA had been raising. IQVIA contends that Veeva "intentionally destroyed swaths of relevant evidence" in what one Veeva employee called "the great data purge." Veeva contends that the "great data purge" refers to employee deletions of records for inactive projects for customers in keeping with Veeva's SOP. IQVIA doubts this explanation, arguing that it does not make sense for Veeva employees to refer to a SOP as a "great data purge." IQVIA also argues that Veeva fails to cite to any evidence that sets forth the alleged SOP.

4. Veeva's Sur-Reply

Veeva reiterates that IQVIA's response to the Shire Incident demonstrates that Veeva had no reason to anticipate litigation at that point in time. Veeva also identifies a June 25, 2016, JIRA ticket that indicates certain data needs "to be purged per our 30 day SOP[,]" as support for its

contention that Veeva had certain SOPs for deleting customer data. Veeva also cites to testimony from Uber that the deletion of certain documents was pursuant to Veeva's clean-up SOP and amounted to the clean up of old project files.

5. IQVIA's Response to Veeva's Sur-Reply

IQVIA argues that Veeva fails to respond to its arguments concerning Veeva's "great data purge" of incriminating evidence in the wake of the Shire Incident. IQVIA also argues that the testimony from Uber refers to a SOP that was created in the lead-up to the E&Y Audit, after most of the deletions in connection with the Genentech Incident.

C. EUStage

1. IQVIA's Arguments

According to IQVIA, the EUStage database was the only source of contemporaneous logs and records that documented Veeva's alleged copying of IQVIA Reference Data offerings in Europe. IQVIA explains that when Veeva began building OpenData in Europe in 2015, it designed a two-part computer system in which Veeva employees would work: (1) an intermediate OpenData database; and (2) a final OpenData database. Each database was stored in a separate "instance" of Veeva Network, Veeva's cloud master data management software. The intermediate OpenData database was stored in an instance called "EUStage." This was the "staging" environment where the database was actually built. The final OpenData database was stored in a separate production instance called "EUMaster."

IQVIA further explains that Veeva Network software has an audit trail that tracks where data in the instance originated. This audit trail includes details such as timestamps showing when Veeva added a specific healthcare provider or organization to OpenData, and labels (keys) indicating its source. Because of the set-up of Veeva's two-part system for OpenData in Europe,

the audit trail was divided between the two instances, with part of the audit trail in EUStage, and the remainder in EUMaster. Thus, IQVIA explains, a complete picture of the audit trail requires access to both EUStage and EUMaster.

IQVIA alleges that in early 2015, Veeva began misappropriating IQVIA Reference Data obtained from mutual clients to build competing offerings in Europe. IQVIA believes that Veeva induced clients to send their existing reference data, which included IQVIA Reference Data, to Veeva so that Veeva could compare it with Veeva's OpenData dataset using the EUStage Network instance. After running this comparison exercise, Veeva would copy the "unmatched" records—i.e., providers or organizations that IQVIA had, but Veeva lacked—into OpenData as new records and mark them for data stewards to "verify" for accuracy.

IQVIA points to an example where, in June 2015, Vincent Pavan, then-Director of EU OpenData Architecture, matched data from client Sobi against Veeva OpenData, describing the Sobi data as "a good quality file from IMS." Pavan loaded that file into EUStage and configured the "match" job such that any healthcare providers in Sobi's IQVIA data that did not exist in Veeva's OpenData would be added as new records and marked for verification. IQVIA explains that this can be illustrated by analyzing a specific record in the Sobi file: an internal medicine resident in France with initials P.C. When Pavan matched the Sobi file on June 8, 2015, Veeva did not have this healthcare provider in OpenData. Just minutes after running the match job, Veeva added this provider to OpenData, assigning the doctor a unique Veeva ID number. Three weeks later, on June 28, 2015, this record was "promoted" into the final EUMaster database.

IQVIA argues that this example illustrates why it needs audit logs, and thus, why its first two document requests in this case requested all "audit logs and similar computer generated documentation" capturing any "data copying, transfer or other computer-based actions"

involving a "comparison" to IQVIA or customer data. IQVIA contends that the Special Master ordered Veeva to produce these requested audit logs in March 2018. Thereafter, IQVIA served a supplemental document request on May 2, 2018, seeking a full disclosure of what audit log information Veeva had available. In Veeva's June 1, 2018, response, it represented that there was no "audit log" that would show "that Veeva performed some sort of special 'data copying' of IQVIA data and/or life sciences company data for purposes of a comparative analysis . . . such as copying that data into Veeva's OpenData database." Just three days later, Veeva marked EUStage for deletion, and then permanently deleted it in August 2018—a year and a half after this lawsuit commenced and after its production was ordered.

IQVIA alleges that Veeva then tried to hide the fact that it deleted EUStage. In March 2019, Veeva made available for inspection two OpenData instances of Veeva Network software (one for the United States and one for Europe) in response to IQVIA's Request for Production ("RFPs") Nos. 1(E) and 2(E). Veeva represented that the two OpenData Network instances would contain "all of the information Veeva has, since the time Veeva began maintaining the OpenData data set." For Europe, however, Veeva only produced a copy of EUMaster.

In July 2019, IQVIA learned for the first time about the deletion of EUStage in connection with the depositions of Veeva employees Vincent Pavan and Ashley Prip. According to IQVIA, Veeva then represented that EUStage had been decommissioned almost a year prior to the lawsuit. During a Rule 30(b)(6) deposition on the issue, Veeva's General Counsel admitted that EUStage was deleted on August 10, 2018 (after being marked for deletion on June 4, 2018). EUStage cannot be restored.

IQVIA asserts that Veeva's deletion of EUStage merits the harshest sanctions. It argues that the evidence cannot be restored or replaced through additional discovery. IQVIA contends

that it has established that EUStage had critical evidence that would prove when and how Veeva incorporated IQVIA's Reference Data (obtained from clients like Sobi) into Veeva's OpenData. That missing evidence goes directly to Veeva's liability for stealing IQVIA's trade secrets. IQVIA argues that while it can demonstrate Veeva's theft with the Sobi-related documents that survived destruction, that spotty evidence concerning a single customer does not cure the prejudice IQVIA suffers from Veeva's destruction of the entire database. IQVIA explains that EUStage was the only source containing definitive proof of when and how Veeva copied IQVIA's Reference Data during the comparison exercises. IQVIA argues that Veeva cannot explain why the timestamps in EUMaster—which obscure Veeva's theft by reflecting dates weeks after the matching exercise occurred in EUStage—provide an adequate substitute.

EUStage had unique information necessary to prove misappropriation that does not exist in EUMaster. IQVIA explains that the "final data" in EUMaster does not contain the critical evidence showing where that data came from and how it was built. IQVIA explains that EUStage contained source indicators that would prove, for example, when Veeva incorporated IQVIA's Reference Data obtained from Sobi (or other clients) into OpenData. The "final data" in EUMaster does not contain this raw source information. Rather than showing records originating from Sobi's file, EUMaster merely shows that the "final data" came from EUStage. Thus, EUStage is required for IQVIA to definitively prove which records in Veeva's OpenData database originated from IQVIA's Reference Data.

IQVIA argues it has been severely prejudiced by Veeva's post-litigation deletion of EUStage. Without EUStage and its critical audit trail, it is impossible for IQVIA to definitively prove which specific records in Veeva's EU OpenData database originated from IQVIA's Reference Data. Likewise, IQVIA argues it has been deprived of evidence that would disprove

Veeva's claims that it built its dataset from legitimate sources, except to the extent it pieces together disparate evidence that survived destruction, like it was able to do with the Sobi-related files. IQVIA argues that lesser sanctions—such as a jury instruction or monetary sanctions—cannot cure this prejudice, as such sanctions do not serve to restore critical evidence in EUStage.

IQVIA believes that the timing of Veeva's deletion of EUStage also clearly establishes Veeva's intent to deprive IQVIA of discovery. Veeva served written discovery responses on June 1, 2018, representing that it did not have audit logs showing that it copied IQVIA's Reference Data into Veeva OpenData. Three days after providing this discovery response, Veeva began the process of permanently deleting EUStage, thus ensuring that IQVIA could not review this critical evidence.

IQVIA argues that Veeva's misstatements about EUStage also establish bad faith. IQVIA explains that in response to IQVIA's request in the fall of 2019 that Veeva make a copy of EUStage available for inspection, Veeva represented that EUStage had been "decommissioned almost a year prior to the lawsuit," and Veeva therefore could not make it available for inspection. Veeva represented that it "cannot produce information [it] [does] not have." IQVIA argues that these statements were blatantly false and that Veeva has now admitted that it deleted EUStage in August 2018. IQVIA asserts that Veeva could not genuinely have believed that, in the midst of this protracted litigation involving heated disputes about the scope of discovery, broad document requests, and Court-ordered preservation instructions, it was nevertheless free to delete a massive database containing the very kind of data at issue in this case—without giving IQVIA or the Court notice and seeking consent.

IQVIA argues that Veeva has produced no evidence demonstrating that EUStage's deletion was during a "company-wide transition to Amazon Web Services." Moreover, IQVIA

argues that EUStage was not deleted in the standard course, rather it was deleted in violation of Veeva's written retention policy, which provides that records relating to Veeva's "Development/Intellectual Property and Trade Secrets" should be kept "[i]ndefinitely." IQVIA asserts that it was a specific request from Veeva's "OpenData team" that prompted the deletion, further demonstrating there was nothing "ordinary" about the deletion of an entire relevant database while this lawsuit was pending.

IQVIA argues that Veeva's deletion of EUStage and its other post-filing deletions and deceptive statements, are particularly egregious and amount to disobeying the Court's orders. IQVIA contends that even if EUStage had been idle since 2016, Veeva still had a duty to preserve it under the Court's October 27, 2017, ESI Order. That Order explicitly prohibited Veeva from destroying "potentially relevant" ESI from "systems no longer in use that cannot be readily accessed."

2. Veeva's Arguments

According to Veeva, EUMaster is the master database in which Veeva keeps its European OpenData product, updates its data (in part by processing data change requests), and sends those updates to its OpenData customers. It contends that EUStage was a short-lived database in which Veeva collected and processed raw data from 2015 to early 2016 before loading it into EUMaster. Veeva asserts that as its data services in Europe improved, it streamlined operations by loading data directly into EUMaster, phasing out EUStage. Veeva explains that once EUStage grew superfluous by February 2016, it was decommissioned. By 2018, the non-functional EUStage database amounted to dead-space in the cloud. Thus, as part of Veeva's global migration of computing infrastructure to Amazon Web Services in 2018, EUStage was deleted.

Veeva argues that to the extent any data stored in EUStage was incorporated into OpenData, details about that incorporation—including the general source information, the date of the incorporation request, and the individual who made the incorporation request—were logged in EUMaster, which Veeva produced. Thus, Veeva argues it has already produced materially similar information by producing EUMaster and various e-mails.

Veeva explains that EUMaster provides details such as "Source Type" and "Created Date." Further, Veeva argues that despite being told that certain raw data processed in EUStage (i.e., the "sources") were archived in a separate repository, the S3 repository, IQVIA never requested production of that repository and instead used the deletion of EUStage to suggest a nefarious cover-up. Veeva also contends that IQVIA never initially requested the EUStage database as its requests for production do not cover EUStage. Veeva further argues that it has already produced approximately one terabyte of other external OpenData/Network software log files.

Veeva thus argues that IQVIA cannot satisfy its burden to show that the routine erasure of EUStage resulted in any prejudice since Veeva already produced the more comprehensive EUMaster database, as well as e-mails documenting specific changes to OpenData that IQVIA allegedly seeks from the EUStage database.

Veeva also argues that IQVIA cannot demonstrate bad faith. Veeva maintains that it never sought to intentionally deceive IQVIA into believing that it deleted EUStage pre-litigation. Veeva argues that if IQVIA were genuinely confused about the distinction between "decommissioning" and "deletion," it could have asked. Moreover, Veeva asserts that IQVIA was obligated to meet and confer with Veeva regarding its confusion. Veeva contends that what

IQVIA denigrates as "false statements" and "ever-changing explanations" amount to misunderstandings on which IQVIA neglected to seek clarification.

D. Google Drive

1. IQVIA's Arguments

According to IQVIA, Google Drive is one of the central repositories in which Veeva stores and manages documents. In connection with the March 2019 deposition of Veeva employee Johnston, IQVIA learned that documents Johnston created or accessed on Google Drive had not been produced. IQVIA followed up with Veeva for these documents and was told that the documents were likely deleted in the ordinary course.

IQVIA then filed a motion to compel Veeva to produce all responsive Google Drive documents and respond to IQVIA's questions about when Google Drive documents were deleted. In opposing the motion, Veeva submitted a sworn declaration from Patrick Young, Veeva's Senior Manager of Global IT Infrastructure. Young's declaration stated that "Veeva uses Google eDiscovery Vault to preserve all Google Drive files, and this system was activated on December 9, 2016." IQVIA argues that such a sworn statement to the Court could not have been made lightly as it went to one of the central issues posed by the motion. The declaration further indicated that Veeva maintains a voluminous number of files on Google Drive, noting that in the last six months, Veeva personnel had added almost 3.4 million files to Google Drive.

Subsequently, in November 2019, Veeva's 30(b)(6) witness on deletion topics, Josh Faddis, testified that Veeva did not begin preserving documents stored on Google Drive until mid-January 2017, around the time IQVIA filed its action. Then, in a January 23, 2020, e-mail, IQVIA was informed that Veeva did not begin preserving Google Drive documents until April 25, 2017. IQVIA asked Veeva for an explanation of these discrepancies and requested that

Veeva provide the official Google Vault report that would show what Veeva actually did to preserve Google Drive documents and when. IQVIA argues that Veeva has refused to provide the report or any further information.

IQVIA argues that Young's lie about when Veeva began preserving Google Drive documents was a central feature of Veeva's opposition to IQVIA's motion to compel Google Drive documents. Veeva submitted Young's false statement after IQVIA demanded information about when documents were deleted from Google Drive. IQVIA believes these facts strongly suggest that Veeva intentionally deceived the Court about when it began preserving Google Drive documents to make IQVIA and the Court credit Veeva's "presum[ption]" that the Google Drive documents were deleted "in the ordinary course."

IQVIA further argues that Veeva's failure to produce evidence that would corroborate its story supports a finding of bad faith. IQVIA argues that it repeatedly requested that Veeva produce a Google Vault audit report, which would include objective, verifiable information regarding, for example, when Veeva put its litigation holds in place on Google Drive, when retention rules were created, and when those retention rules were changed, among many other relevant data points. IQVIA maintains that Veeva has only produced excerpts of the Google Vault audit report and not the entire report. It explains that Veeva has only provided an e-mail from its counsel containing a short "chart," with a few cherry-picked snippets purportedly regarding the "preservation for Google Drive." Veeva did not produce the full Google Vault audit report that IQVIA requested and IQVIA believes this raises questions about what Veeva is trying to hide, especially after it has already lied in sworn testimony.

Thus, IQVIA argues that incriminating Google Drive documents could have been deleted for months after litigation was filed. IQVIA explains that Google Drive is central to the conduct

of Veeva's business and points to the Young declaration which stated that Veeva personnel had added almost 3.4 million files to Google Drive in a six month period. Moreover, IQVIA argues that Veeva has acknowledged that Google Drive was "likely to contain non-duplicative information relevant to this action." IQVIA argues that the fact that Veeva has produced some subset of documents from its Google Drive cannot absolve Veeva of its failure to preserve Google Drive documents post-litigation.

2. Veeva's Arguments

Veeva explains that after IQVIA filed suit in January 2017, it instituted litigation hold measures for IT systems within Veeva, including Salesforce.com, Egnyte, Confluence, Zendesk, JIRA, and key Veeva Vault instances (Marketing, QMS, Sales, Services, and Clinical Operations). Veeva also worked to archive all communications circulated among Veeva's Google applications by installing Google Vault. As Veeva's 30(b)(6) witness testified, Google Vault "ignores the employee's action, and it takes everything—every transaction that's happened in the employee's inbox is captured, no matter what the employee does locally. That's the purpose of Google Vault."

As for the Google Drive documents, Veeva believed that its litigation hold had covered all Google applications. Veeva later determined that Google Drive was not included in the original hold used to preserve Google e-mail and chat sessions—in part because Google did not offer such hold functionality for Google Drive until March 2017—and promptly cured its oversight in April 2017. Despite this misstep, Veeva argues that it produced approximately 63,000 Google Drive documents and identified nothing to suggest that any relevant documents were deleted from January to April 2017. Veeva argues that any non-preservation of Google

Drive documents was inadvertent and inflicted no prejudice on IQVIA. Thus, it argues that no sanctions are warranted.

With respect to the Young declaration, Veeva explains that Young was not personally involved in implementing the litigation hold and mistakenly represented that Veeva began preserving Google Drive documents before April 2017. Young made his representation in good faith, as he relied on the date on which Veeva began subscribing to Google Vault, a program Veeva used to automatically archive Google-stored materials. Young was unaware that, although Veeva began archiving Gmail and Google Chat records in January 2017, Vault functionality was not available for Google Drive until two months later in March 2017.

Veeva explains that Young was not the only person confused about Google Vault's changing services: Veeva's Chief Information Officer at the time, Prasad Ramakrishnan, was likewise unaware that Google did not offer the "Vault" functionality for Google Drive until March 2017, and he belatedly activated the function for Google Drive in April 2017. Veeva argues that Ramakrishnan's mistake cannot elicit sanctions.

Veeva believes that the record is clear that there was at most a slight, good-faith, and harmless delay in preserving Veeva's Google Drive materials. It further argues that preservation delays do not warrant any sanctions, let alone case-terminating ones. Veeva also asserts that it has turned over a copy of the Google Vault audit report, which it maintains IQVIA attached it to its own motion. Moreover, Veeva argues that any purported prejudice was minimal, as Veeva produced approximately 63,000 documents from Google Drive.

E. James Kahan E-mails

1. Background

James Kahan began working at Veeva in June 2013 as Senior Director of Veeva OpenData. IQVIA alleges that Veeva's misappropriation of IQVIA's Reference Data began as early as June 2013, when Kahan began to build OpenData.

In February 2019, IQVIA requested that Veeva add Kahan as a custodian, collect his documents, apply technology assisted review ("TAR"), and produce relevant and responsive documents. At the June 4, 2019, status conference before the Special Master, Veeva did not contest Kahan's relevancy to the lawsuit, but rather, requested that he be added as a custodian at a later date, explaining that adding Kahan as a custodian was a big job. The Special Master saw no reason to delay having Kahan added as a custodian. Veeva then added Kahan as a custodian and completed its production of Kahan's documents on September 2, 2019. IQVIA contends that it immediately noticed a major gap in Kahan's e-mails, from January 2014 through May 2015, which coincided with the crucial period when he served as the Senior Director responsible for Veeva OpenData.

According to Veeva's 30(b)(6) deposition of Faddis, Kahan's Google e-mails were "vaulted" when Veeva subscribed to Google Vault around the time this action was initiated. Veeva undertook an investigation to determine if any of Kahan's e-mails were deleted. Veeva determined that Corporate IT did not initiate a deletion.

Kahan testified that nearly all of his e-mails from 2014 were deleted. He did not know who deleted them and he was only made aware of the deletion in preparation for his deposition. Kahan explained that "during that period of time, however, there were storage limits per account on e-mails. And as somebody who received a large number of e-mails with very large

attachments I would reach that limit on a somewhat regular basis. In order to continue to be able to receive e-mails I would have to reduce my storage by deleting e-mails and it is entirely possible that that is what was going on during that period of time." However, Kahan confirmed that he had no personal knowledge of when the e-mails were deleted, how they were deleted, or by whom they were deleted.

2. IQVIA's Arguments

According to IQVIA, the record establishes that Kahan's e-mails were deleted sometime after September 23, 2015, because later documents produced in the case show that Kahan was able to look back through the now-deleted e-mails as of that time. IQVIA argues that because Veeva anticipated litigation with IQVIA no later than September 25, 2015, Veeva's subsequent deletion of Kahan's e-mails constitutes spoliation, no matter the precise date they were purged. IQVIA argues that Veeva's duty to preserve potentially relevant evidence began in September 2015 when Veeva's preparations for the E&Y Audit revealed its theft of IQVIA's data and Veeva anticipated litigation as a result.

IQVIA argues the Kahan e-mails cannot be restored or replaced through additional discovery. IQVIA contends that the limited production of some e-mails from other custodians that happened to copy Kahan does not cure the fact that Veeva destroyed a significant amount of evidence from the e-mails of Kahan. IQVIA explains that not only is it unable to trace the contribution of IQVIA Reference Data to Veeva OpenData as a result of Veeva's deletions in HDM, IQVIA likewise cannot even review Kahan's contemporaneous custodial e-mails from this same time period, as Veeva deleted them as well. Thus, it argues the threshold requirement is plainly satisfied.

With respect to intent, IQVIA argues that while Veeva claims it does not know who deleted Kahan's e-mails, it has never suggested the deletion was inadvertent. Moreover, IQVIA argues that the deletion of the Kahan e-mails was against Veeva's stated policy. With respect to Veeva's assertions that the e-mails were likely deleted due to storage constraints, IQVIA points to the deposition of Eric Davis, another OpenData employee, who testified that he had never heard anyone at Veeva discuss storage issues related to e-mail and did not recall any storage limitation that would require him to delete an e-mail. IQVIA also argues that the IT tickets that Veeva cites—one from October 2014, one from February 2016, and two from September 2015—relating to employees in non-OpenData divisions of the company requesting additional e-mail storage, say nothing about what happened to Kahan's e-mails from January 2014 to May 2015. Moreover, IQVIA argues that these examples illustrate that Veeva simply increased the Gmail space available for these employees.

IQVIA believes the purpose of Veeva's deletion was clearly to conceal its misappropriation of IQVIA's Reference Data. IQVIA argues that the fact that Veeva cannot explain when it deleted Kahan's e-mails is also highly suspicious. IQVIA further argues it has repeatedly asked Veeva to produce a Google Vault report that would potentially verify Veeva's assurances that it configured Google Vault to start retaining all employee e-mails in January 2017 in connection with the litigation hold implemented for this case. Veeva has not provided that report.

3. Veeva's Arguments

Veeva argues that it did not intentionally delete Kahan's e-mails from January 2014 to May 2015 after its duty to preserve arose. It argues it has produced 6,800 of Kahan's e-mails from that 17-month period. Veeva explains that Kahan's 2014-2015 e-mails were collected from

the mailboxes of other custodians. Veeva further argues that it produced approximately 65,000 e-mails from Kahan's files outside that period, including long before Veeva bore any obligation to preserve them. Veeva asserts that any deletions of Kahan's e-mails were done years ago for a humdrum reason: to free up space on Kahan's mailbox due to a system-imposed, per user mailbox storage limit. Thus, Veeva argues that any deletions were done pre-litigation before its duty to preserve arose. Veeva further argues that any culling of old e-mails was innocuous. Veeva argues that even if it had anticipated litigation in September 2015, sanctions still would be unwarranted because IQVIA cannot demonstrate the relevance of the e-mails and because Veeva has produced other materials to substitute for the lost e-mails. Therefore, IQVIA has suffered no harm or prejudice.

Veeva argues that there is no reason to assume that Kahan's missing e-mails are the result of the intentional destruction of evidence. Rather, Veeva points out that both Kahan and Veeva's 30(b)(6) witness supplied a reasonable and innocuous explanation, that Kahan reached a system-imposed, per user mailbox storage size limit. Veeva thus argues that to the extent Kahan's January 2014–May 2015 e-mails were removed, the purpose was to free space in Kahan's mailbox—not to intentionally deprive IQVIA of evidence.

With respect to other employees who had their storage limits increased, Veeva argues this says nothing about how Kahan coped with his e-mail storage issues, particularly where Kahan testified that his receipt of "very large attachments" through e-mail compelled him to "reduce [his] storage by deleting e-mails." Veeva argues that it is IQVIA's burden to prove bad faith, not Veeva's burden to refute it. *Bull v. United Parcel Serv.*, 665 F.3d 68, 76–77 (3d Cir. 2012)

III. Applicable Law

"Spoliation is 'the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonable foreseeable litigation.'" *Bensel v. Allied Pilots Ass'n*, 263 F.R.D. 150, 152 (D.N.J. 2009) (citing *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir. 1999)). "Spoliation sanctions serve a remedial function by leveling the playing field or restoring the prejudiced party to the position it would have been without spoliation." *Mosaid Techs. Inc. v. Samsung Elecs. Co.*, 348 F. Supp. 2d 332, 335 (D.N.J. 2004). Spoliation sanctions "also serve a punitive function, by punishing the spoliator for its actions, and a deterrent function, by sending a clear message to other potential litigants that this type of behavior will not be tolerated and will be dealt with appropriately if need be." *Id.* at 335.

Whether to grant or deny a motion for discovery sanctions is generally committed to the sound discretion of the District Court. *See e.g.*, *Clientron Corp. v. Devon IT, Inc.*, 894 F.3d 568, 577 (3d Cir. 2018) (citing *McLaughlin v. Phelan Hallinan & Schmieg, LLP*, 756 F.3d 240, 248 (3d Cir. 2014)). Prior to the imposition of sanctions for spoliation, the Court must initially determine "whether the duty to preserve evidence has been triggered." *Kounelis v. Sherrer*, 529 F. Supp. 2d 503, 518 (D.N.J. 2008). "An independent duty to preserve relevant evidence arises when the party in possession of the evidence knows that litigation by the party seeking the evidence is pending or probable and the party in possession of the evidence can foresee the harm or prejudice that would be caused to the party seeking the evidence if the evidence were to be discarded." *Id.*; *see also Bensel v. Allied Pilots Ass'n*, 263 F.R.D. 150, 152 (D.N.J. 2009) ("While there is no duty to keep or retain every document in the party's possession, 'even in advance of litigation, it [a party] is under a duty to preserve what it knows or reasonabl[y] should know, will likely be requested in reasonably foreseeable litigation.'") (citation omitted); *see also*

Fed. R. Civ. P. 37(e), Advisory Committee Note to 2015 Amendment ("Rule 37(e) does not purport to create a duty to preserve. The new rule takes the duty as it is established by case law, which uniformly holds that a duty to preserve information arises when litigation is reasonably anticipated.").

Once a party reasonably anticipates or knows of pending litigation and the duty to preserve has attached, a party "must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents." *Sanofi-Aventis Deutschland GmbH v. Glenmark Pharm. Inc.*, No. 07-CV-5855, 2010 WL 2652412, at *3 (D.N.J. July 1, 2010) (citing *Major Tours, Inc. v. Colorel*, No. 05-3091, 2009 WL 2413631, at *2 (D.N.J. Aug. 4, 2009)); *see also Crown Castle USA Inc. v. Fred A. Nudd Corp.*, No. 05-CV-6163T, 2010 WL 1286366, at *10 (W.D.N.Y. Mar. 31, 2010)("Once the duty to preserve has attached, a party should institute a litigation hold and 'suspend its routine document and retention/destruction policy.'") (citation omitted). Where "the duty to preserve evidence has not been triggered at the time the evidence was destroyed, then there can be no spoliation." *Kounelis*, 529 F. Supp. 2d at 518.

Rule 37(e), as revised by the December 1, 2015, amendments, specifically addresses the applicability of sanctions for spoliation of Electronically Stored Information ("ESI"). Sanctions for spoliation of ESI pursuant to Rule 37(e) requires a two-step analysis. First, the court must determine if spoliation of evidence occurred, and second, the court must determine which sanction is appropriate. "'Where the amended rule applies, it provides the exclusive remedy for spoliation of electronically stored information ('ESI'), foreclosing reliance on the court's inherent authority.'" *Martin v. Wetzel*, No. 1:18-CV-00215-RAL, 2020 WL 6948982, at *2

(W.D. Pa. Nov. 25, 2020)(quoting *Bistrian v. Levii*, 448 F. Supp. 3d 454, 464 (E.D. Pa. 2020) (citing Fed. R. Civ. P. 37(e) Advisory Committee's Note to 2015 amendment)).

Rule 37(e), governing sanctions for a party's failure to preserve ESI, provides as follows:

> (e) Failure to Preserve Electronically Stored Information. If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:
>
> (1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or
>
> (2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:
>
> (A) presume that the lost information was unfavorable to the party;
>
> (B) instruct the jury that it may or must presume the information was unfavorable to the party; or
>
> (C) dismiss the action or enter a default judgment.

Accordingly, for the Special Master to first make a finding that spoliation occurred pursuant to this Rule, IQVIA must show: (1) that certain ESI should have been preserved in anticipation of litigation; (2) that ESI was lost; (3) the ESI was lost because Veeva failed to take reasonable steps to preserve it; and (4) that it cannot be restored or replaced. *See Goldrich v. City of Jersey City*, No. CV 15-885 (SDW)(LDW), 2018 WL 4492931, at *7 (D.N.J. July 25, 2018), report and recommendation adopted as modified, 2018 WL 4489674 (D.N.J. Sept. 19, 2018).

Next, to determine the appropriate sanctions to be imposed, the Special Master must find either prejudice to IQVIA or that Veeva acted with the intent to deprive IQVIA of the ESI's use in the litigation. Upon either finding, when deciding which sanction to impose, the Special Master should consider: "(1) the degree of fault of the party who altered or destroyed the evidence; (2) the degree of prejudice suffered by the opposing party; and (3) whether there is a

lesser sanction that will avoid substantial unfairness to the opposing party and ... deter such conduct by others in the future." *Id.* (quoting *Capogrosso v. 30 River Court E. Urban Renewal Co.*, 482 F. App'x 677, 682 (3d Cir. 2012); *see also Schmid v. Milwaukee Elec. Tool Corp.*, 13 F.3d 76, 79 (3d Cir. 1994). The burden is on the moving party "to show that spoliation occurred and what sanctions are appropriate." *Fuhs v. McLachlan Drilling Co.*, No. 16-376, 2018 WL 5312760, at *13 (W.D. Pa. Oct. 26, 2018) (quoting *Goldrich*, 2018 WL 4492931 at *7.

As discussed above, sanctions for spoliation pursuant to Rule 37(e)(1) require a finding of prejudice to another party from loss of the information. "[P]rejudice exists where documents that are relevant to a claim are unavailable and the moving party has come forward with a plausible, good faith suggestion as to what the evidence might have been." *Goldrich*, 2018 WL 4492931 at *10 (citing *Schmid*, 13 F.3d at 80). The 2015 Advisory Committee Notes to Rule 37(e) explain that "[a]n evaluation of prejudice from the loss of information necessarily includes an evaluation of the information's importance in the litigation." 2015 Advisory Committee Notes to Rule 37(e).

Rule 37(e)(2) sanctions do not require the court to find prejudice to the party deprived of the information. Rather, sanctions pursuant to Rule 37(e)(2) require a finding of intent, which supports an inference that the lost information was unfavorable to the party that intentionally destroyed it and that the opposing party was prejudiced by the loss of the information. *See* 2015 Advisory Committee Notes to Rule 37(e).

With respect to sanctions available pursuant to Rule 37(e)(2), "[d]ismissal or suppression of evidence are the two most drastic sanctions because they strike at the core of the underlying lawsuit." *Mosaid Techs. Inc.*, 348 F. Supp. 2d at 335. A court may issue a dispositive sanction where the innocent party's case is "severely impaired because it lacked the information that was

not produced." *GN Netcom, Inc. v. Plantronics, Inc.*, 930 F.3d 76, 82 (3d Cir. 2019) (quoting *Bull*, 665 F.3d at 83). Before entering a default judgment sanction, courts typically also conduct a "Poulis analysis," *Knoll v. City of Allentown*, 707 F.3d 406, 409 (3d Cir. 2013), which entails the consideration of

> (1) the extent of the party's personal responsibility; (2) the prejudice to the adversary caused by the failure to meet scheduling orders and respond to discovery; (3) a history of dilatoriness; (4) whether the conduct of the party or the attorney was willful or in bad faith; (5) the effectiveness of sanctions other than dismissal, which entails an analysis of alternative sanctions; and (6) the meritoriousness of the claim or defense.

Poulis v. State Farm Fire & Cas. Co., 747 F.2d 863, 868 (3d Cir. 1984) (emphasis deleted).

One lesser sanction is an adverse jury instruction. A jury instruction on the spoliation inference permits the jury to infer "that the destroyed evidence might or would have been unfavorable to the position of the offending party." *Scott v. IBM Corp.*, 196 F.R.D. 233, 248 (D.N.J. 2000), as amended (Nov. 29, 2000) (declining to exercise the court's inherent sanctioning powers, but considering as a "second inquiry ... whether the[ ] circumstances of spoliation, although not rising to the level of sanctionable conduct, should nevertheless give rise to a jury instruction regarding the spoliation inference."). "When the contents of a document are relevant to an issue in the case, the spoliation inference is nothing more than the common sense observation that a party who destroys relevant evidence did so out of a well-founded fear that the contents would harm him." *Id.* (citing *Brewer v. Quaker State Oil Ref. Corp.*, 72 F.3d 326, 334 (3d Cir. 1995)).

Courts have employed a four-factor test to determine whether an adverse inference jury instruction is appropriate. *Mosaid Techs. Inc.*, 348 F. Supp. 2d at 336. These factors are: (1) the destroyed evidence must be within the offending "party's control ...;" (2) "it must appear that

there has been actual suppression or withholding of the evidence ...;" (3) the "evidence destroyed or withheld was relevant to the claims or defenses;" and (4) "it was reasonably foreseeable that the evidence would later be discoverable." *Id.* (citations omitted); *see also Kounelis*, 529 F. Supp. 2d at 520.

IV. Opinion

A. Genentech Incident

The Special Master finds that Veeva should have anticipated litigation with IQVIA in September 2015, and therefore, had a duty to preserve evidence at that time. Prior to the imposition of sanctions for spoliation, the Court must initially determine "whether the duty to preserve evidence has been triggered." *Kounelis*, 529 F. Supp. 2d at 518. "An independent duty to preserve relevant evidence arises when the party in possession of the evidence knows that litigation by the party seeking the evidence is pending or probable and the party in possession of the evidence can foresee the harm or prejudice that would be caused to the party seeking the evidence if the evidence were to be discarded." *Id.* Veeva was well aware of IQVIA's concerns that Veeva might improperly use its access to IQVIA Reference Data to build its competing data offering, OpenData. Indeed, the purpose of the E&Y Audit was to evaluate Veeva's security measures and assurances. It is undisputed that, in preparing for the audit, Veeva uncovered the Genentech Incident, which involved a configuration error that programmatically included IQVIA address records as a source in Veeva's "best address" algorithm to verify address records in OpenData. Additionally, the database storing these records was viewable by Veeva's OpenData data stewards, who were responsible for improving and maintaining Veeva OpenData.

Veeva argues that the Genentech Incident did not give rise to an anticipation of litigation because it was minor and swiftly rectified. Veeva also argues that the Genentech Incident was

unrelated to the E&Y Audit because it involved a different database. The Special Master finds these arguments unpersuasive. Initially, if the Genentech Incident was unrelated to the E&Y Audit, there would have been no reason to delay the audit in the first instance. Furthermore, the OpenData Data Corruption Memo,[10] which was prepared by Veeva employees in response to the Genentech Incident, specifically finds that the E&Y Audit would uncover the Genentech Incident, and therefore, Veeva needed to delay the audit in order to rectify the situation. In addition, although Veeva contends that the Genentech Incident was "minor" because it only involved 1,350 address records out of more than 10 million OpenData records, its own internal communications and documents suggest that it was not so minor. Many high level Veeva employees voiced concern over the gravity of the situation and IQVIA's anticipated response. The OpenData Data Corruption Memo contemplates that IQVIA will file a lawsuit as a result of the Genentech Incident and that Veeva's exposure could be high. Veeva employees were instructed to avoid using key words relating to IQVIA in e-mail discussions on the Genentech Incident, and to delete chats and stop e-mailing on the subject. Moreover, IQVIA argues that Veeva identified nine other customers with the same issue, but Veeva does not include any data regarding these customers because it was unable to confirm whether they included IQVIA data. Veeva fails to address this argument. There can be no question that Veeva could foresee the harm or prejudice to IQVIA if the evidence were to be lost or discarded. The extent and sufficiency of Veeva's safeguards to prevent the misappropriation of IQVIA Reference Data was at the forefront of discussions and negotiations between the parties concerning the interplay of their offerings.

[10] The Special Master has overruled Veeva's assertion of privilege over this document. Therefore, the Special Master considers it in connection with IQVIA's Sanctions Motion.

Veeva also argues that it had no reason to anticipate litigation with IQVIA at the time of the Genentech Incident, because of the manner in which IQVIA responded to the Shire Incident some eight months later. Specifically, Veeva contends that in both instances, it inadvertently accessed IQVIA data without its authorization. Veeva further contends that when it discussed the Shire Incident with IQVIA, IQVIA did not threaten litigation and thanked Veeva for promptly deleting the data. The Special Master is unpersuaded by this argument. Initially, had IQVIA been aware of the Genentech Incident, it may have reacted very differently to the Shire Incident. Furthermore, the Genentech Incident occurred immediately prior to a third-party audit that was specifically searching for and would have unearthed Veeva's misappropriation. To avoid that outcome, Veeva delayed the audit and engaged in an extensive clean-up endeavor to hide what had occurred. In addition, after the Shire Incident, Veeva made assurances to IQVIA that the data was promptly deleted, and was not retained, used or viewable by any Veeva personnel. Veeva cannot say the same for the Genentech Incident. Thus, comparing the two instances and IQVIA's reaction is improper.

Once a party reasonably anticipates or knows of pending litigation and the duty to preserve has attached, a party "must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents." *Sanofi-Aventis Deutschland GmbH*, 2010 WL 2652412 at *3. Here, after discovering the extent of the Genentech Incident, and identifying the likelihood of litigation as a result thereof, rather than begin to preserve relevant evidence and suspend document destruction policies, Veeva actively and purposefully deleted evidence relating thereto. Veeva first delayed the E&Y Audit, knowing that the audit would likely uncover the Genentech Incident. It instructed employees to either

delete communications about the Genentech Incident, or to avoid the use of keywords relating to IQVIA in communications on the subject matter.

In addition, IQVIA contends that Veeva further deleted over two hundred directories on its NAS server, thousands of tables within its HDM database, and over one thousand DVI tables. Veeva does not appear to dispute that it deleted this evidence, but rather contends that the deleted data is irrelevant to IQVIA's trade secret claims. Veeva also contends that much of the allegedly "deleted" materials were recovered and produced in discovery. Veeva states that it "recovered and produced from its comprehensive e-mail searches attachments that included data removed from NAS and HDM." Specifically, Veeva cites to certain customer data that survived its deletion efforts. (Veeva Opp. Br. at p. 39 n.123). IQVIA responds that Veeva has failed to demonstrate any overlap between the subset of data extracts that Veeva produced in discovery and the data that Veeva deleted from HDM. IQVIA argues that the eight customer data extracts that Veeva cites in footnote 123, on page 39 of its Opposition, does not cover the 200 NAS directories and thousands of tables and databases deleted from HDM. Thus, IQVIA contends that the subset of data extracts that Veeva produced are in no way a substitute for the data that Veeva deleted from HDM. The Special Master agrees.

The Special Master finds that the deleted evidence is relevant, particularly because Veeva cites to the absence of such evidence to argue that IQVIA cannot prove that Veeva engaged in trade-secret theft. Furthermore, because of Veeva's deletion of the evidence, IQVIA is unable to recreate what happened and determine the full scope of the misappropriation. The aforementioned evidence should have been preserved in anticipation of litigation, such evidence has been lost, and the evidence was lost because Veeva failed to take reasonable steps to preserve it. The Special Master further finds that the information contained in these repositories

is not recoverable and cannot be restored or replaced by other discovery. Thus, the Special Master finds that spoliation has occurred.

Next, to determine the appropriate sanction for spoliation, the Special Master considers whether IQVIA is prejudiced by the loss of the ESI and whether Veeva acted with intent to deprive IQVIA of the information's use in the litigation. IQVIA asks the Special Master to enter default judgment as to Veeva's liability on IQVIA's claims and dismiss Veeva's counterclaims, or alternatively, impose an adverse inference. As discuss above, sanctions for spoliation pursuant to Rule 37(e)(1) requires a finding of prejudice to another party from loss of the information. Upon a finding of such prejudice, courts are permitted to order measures "no greater than necessary" to cure the prejudice. Courts have found prejudice exists where documents that are relevant to a claim are unavailable and the moving party has come forward with a plausible, good faith suggestion as to what the evidence might have been. *See GN Netcom, Inc. v. Plantronics, Inc.*, No. 12-cv-1318, 2016 WL 3792833, at *6 (D. Del. July 12, 2016); *Schmid*, 13 F.3d at 80. The Special Master finds that IQVIA has demonstrated that it is prejudiced by the deletion of data from Veeva's NAS server, HDM database, and DVI tables. IQVIA has come forward with a plausible, good faith suggestion as to what the deleted evidence would have shown – particularly how and to what extent IQVIA Reference Data may have been used to improve Veeva OpenData. The deleted ESI bears directly on IQVIA's ability to prove its claims and defenses.

Sanctions for spoliation pursuant to Rule 37(e)(2) do not require the court to find prejudice to the party deprived of the information. Rather, sanctions pursuant to Rule 37(e)(2) require a finding of intent, which supports an inference that the lost information was unfavorable to the party that intentionally destroyed it and that the opposing party was prejudiced by the loss

of information. *See* 2015 Advisory Committee Notes to Rule 37(e). Here, the Special Master finds that Veeva acted with the requisite intent to deprive IQVIA of the evidence set forth above. Although Veeva attempts to minimize the Genentech Incident, its conduct and the sentiment of many of its employees indicates just how concerning it was. As set forth above, Veeva twice delayed the E&Y Audit to further investigate and respond to the Genentech Incident. It conducted an internal investigation that revealed the severity of the misappropriation and engaged in multiple meetings and communications to determine how to respond to the incident. The OpenData Data Corruption Memo indicates that Veeva was well-aware that it was misappropriating IQVIA data, something the E&Y Audit would uncover, and that the incident could lead to litigation. Rather than disclose the allegedly "minor" Genentech Incident to IQVIA or the auditors, Veeva chose to cover it up, deleting evidence and directing employees not to create further evidence on the subject (such as replacing "IMS" with "***" in e-mails, not discussing the situation in chats or e-mails, and deleting chats or e-mails where the incident was discussed).

Having found that IQVIA is prejudiced pursuant to Rule 37(e)(1) and finding that Veeva had the requisite intent pursuant to Rule 37(e)(2), the Special Master considers which sanctions to impose. Potential sanctions for spoliation include: "dismissal of a claim or granting judgment in favor of a prejudiced party; suppression of evidence; an adverse inference, referred to as the spoliation inference; fines; and attorneys' fees and costs." *Mosaid Techs. Inc.*, 348 F. Supp. 2d at 335 (internal citations omitted). Sanctions are appropriate where there exists evidence that a party's spoliation threatens the integrity of the court. *Id.* Spoliation sanctions serve a remedial function – to level the playing field – as well as a punitive and deterrent function – to punish the spoliator for its conduct and send a clear message to other potential litigators that such conduct

will not be tolerated. *Id.* Dismissal and the suppression of evidence are two of the most drastic sanctions and will only be imposed in the most extraordinary of circumstances. *Id.* In determining whether the present situation is one of those extraordinary circumstances, the Special Master considers "(1) the degree of fault of the party who altered or destroyed the evidence; (2) the degree of prejudice suffered by the opposing party; and (3) whether there is a lesser sanction that will avoid substantial unfairness to the opposing party and, where the offending party is seriously at fault, will serve to deter such conduct by others in the future." *GN Netcom, Inc.*, 930 F.3d at 82 (quoting *Schmid*, 13 F.3d at 79).

A far lesser sanction is the spoliation inference, which is an adverse inference that allows the jury to infer that the destroyed evidence would have been unfavorable to the spoliating party. *Id.* at 335-36. In order for the spoliation inference to apply, IQVIA must satisfy four elements: (1) the evidence in question was within Veeva's control; (2) there was actual suppression or withholding of the evidence; (3) the evidence destroyed or withheld was relevant to the claims or defenses; and (4) it is reasonably foreseeable that the evidence would later be discoverable. *Id.* at 336. Although a litigant is not required to preserve all documents in its possession in advance of litigation, it is under a duty to preserve what it knows, or reasonably should know, will be requested in reasonably foreseeable litigation. *Id.*

Here, the Special Master concludes that the appropriate sanction for spoliation is an adverse inference charge. Thus, the Special Master recommends that the District Court allow IQVIA to present evidence to the jury regarding the loss of evidence and to issue an adverse inference jury instruction that it deems fit to assist in the jury's evaluation of such evidence. Although the Special Master is concerned with Veeva's conduct, dismissal or suppression of evidence are the two most drastic sanctions and are to be used only in the most extraordinary of

circumstances. *Mosaid Techs. Inc.*, 348 F. Supp. 2d 335. The Special Master concludes that while Veeva's degree of fault is high, and IQVIA's degree of prejudice is also high, a lesser sanction is available that will avoid substantial unfairness and deter conduct in the future. "A dispositive sanction is warranted only where the non-responsible party's case is severely impaired because it lacked the information that was not produced." *GN Netcom, Inc.*, 930 F.3d at 82. The Special Master finds that IQVIA has been able to present a persuasive and compelling case despite the absence of the foregoing evidence. Thus, case-terminating sanctions are unwarranted.

B. Shire Incident

As set forth above, the Special Master has determined that Veeva should have anticipated litigation with IQVIA in September 2015. Once a party reasonably anticipates or knows of pending litigation and the duty to preserve has attached, a party "must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents." *Sanofi-Aventis Deutschland GmbH*, 2010 WL 2652412 at *3. The Shire Incident occurred in May 2016. Thus, at the time of the Shire Incident, Veeva was under a duty to preserve relevant evidence.

Initially, the Special Master does not find the Shire Incident to be substantially similar to the Genentech Incident, mainly because in the Shire Incident, Veeva certified and affirmed to IQVIA that "no extracted data was contributed to Veeva OpenData[.]" However, quite the opposite occurred in the Genentech Incident. Although Veeva attempts to minimize the quantity and import of the IQVIA data that it misappropriated in connection with the Genentech Incident, there is no dispute that IQVIA Reference Data was "programmatically" included in Veeva OpenData. Thus, to suggest that IQVIA's response to the Shire Incident somehow provides

insight on how IQVIA would have responded to the Genentech Incident, had it known about it, or justifies Veeva's conduct in connection with the Genentech Incident, is misguided. Moreover, IQVIA ultimately filed a lawsuit in part because of the Shire Incident.

Notwithstanding, it is not entirely clear to the Special Master, based on the briefing, what evidence was allegedly destroyed as a result of the Shire Incident and how that evidence is relevant to IQVIA's case. To prove spoliation, IQVIA must show that there was actual suppression or withholding of "relevant" evidence. *Bull*, 665 F.3d at 73. IQVIA cites to certain chats, which Veeva employees were instructed to delete, after discussing the Shire Incident. However, the chats were produced in discovery, therefore, they were not spoliated. Furthermore, IQVIA cites to certain documents that Veeva employees were unable to locate and believed must have gotten caught up in the "great data purge." It is unclear to the Special Master what the missing documents are and how they are relevant to IQVIA's claims. Moreover, it is undisputed that Veeva deleted the customer extract that it received from Shire. It certified to IQVIA that the information contained in that extract was not used in Veeva OpenData. Based on the briefing, it is unclear if IQVIA is disputing whether the Shire customer extract, which contained IQVIA Reference Data, was misappropriated and contributed to OpenData. Thus, because it is unclear what relevant evidence was purportedly destroyed in connection with the Shire Incident, the Special Master makes no finding of spoliation at this time.

C. EUStage

The Special Master finds that spoliation did occur when Veeva failed to preserve EUStage. There is no dispute that EUStage was permanently deleted on August 10, 2018, over a year and a half after IQVIA filed suit in this matter. There is also no dispute that EUStage contained evidence that was relevant to IQVIA's claims and defenses. Veeva appears to argue

that as EUStage had been inactive or "decommissioned" since February 2016 it was under no duty to preserve it.

First, the Special Master notes that the ESI Order entered in this case on October 27, 2017, specifically provides: "No ESI or backup media created or received prior to January 1, 2010 will be preserved. The parties agree to preserve all other ESI that they in good faith believe may be potentially discoverable in this matter." (ECF 93). With respect to "systems no longer in use that cannot be readily accessed" the ESI Order states that those sources would "be preserved but not searched." *Id.* To the extent a party believed information from any systems no longer in use was necessary, the parties were to meet and confer on a case-by-case basis. *Id.*

Second, the Special Master notes that IQVIA's RFPs Nos. 1(E) and 2(E), dated September 12, 2017, sought audit logs reflecting any copying, transfers or other computer-based actions involving various IQVIA data. RFP No. 1(E) requested:

> All documents concerning any proposed, actual or contemplated evaluation, analysis, discussion, comparison or review of any Healthcare Professional Data, Reference Data, Sub-National Information or Sales Data obtained from a life sciences company, including but not limited to: (E) All audit logs and similar computer generated documentation reflecting any data copying, transfers or other computer-based actions involving any such data and each individual machine and user accessing such data[.]

RFP No. 2(E) requested:

> All documents concerning any proposed, actual or contemplated evaluation, analysis, discussion, comparison or review of any IMS Market Research Offerings, including but not limited to: (E) All audit logs and similar computer generated documentation reflecting any data copying, transfers or other computer-based actions involving any such data and each individual machine and user accessing such data[.]

The Special Master also notes that in his March 28, 2018, Order and accompanying Opinion, he granted IQVIA's request to compel Veeva to respond to RFP Nos. 1 and 2, and directed Veeva to fully respond by providing full and complete responses to the best of its ability. (ECF 115, 116). Thus, the Special Master finds that audit logs from Veeva networks were requested by IQVIA and that Veeva should not have deleted EUStage in light of the ESI Order entered in this case.

The Special Master further finds that the information contained in EUStage is not recoverable and cannot be replaced by other discovery. IQVIA has amply demonstrated how the audit trail in EUStage contained critical evidence that would have allowed it to piece together examples of how Veeva utilized report card comparison exercises to obtain IQVIA data which it then utilized to improve its own OpenData product. Veeva points to *In re Pfizer Inc.*, 288 F.R.D. 297, 324 (S.D.N.Y. 2013), to argue that sanctions are not warranted because it provided an adequate substitute. However, the Special Master is not persuaded by Veeva's arguments that it produced an adequate substitution for the evidence contained in EUStage by producing EUMaster and various e-mails documenting specific changes to OpenData. The final data in EUMaster does not contain the raw source information IQVIA requires to support its claims. Moreover, Veeva has not described how the e-mails it produced may be a sufficient substitute for the audit trails, which have been lost.

Additionally, Veeva's assertion that certain raw data processed in EUStage has been archived in the S3 repository is both vague and unconvincing. Veeva has not detailed what specific raw data that was processed in EUStage is available in the S3 repository and in light of Veeva's ambiguous assertions the Special Master cannot understand what information is contained in the S3 repository and cannot find that the S3 repository is an adequate substitution

for the audit trails lost due to the deletion of EUStage. Moreover, if the S3 repository did contain the audit trail information IQVIA first requested in September 2017, the Special Master cannot understand why this information has not already been produced. Thus, the Special Master finds that EUStage (1) should have been preserved in anticipation of litigation; (2) that evidence was lost; (3) the ESI was lost because Veeva failed to preserve it; and (4) that it cannot be restored or replaced.

Next, to determine the appropriate sanction for spoliation, the Special Master considers whether IQVIA is prejudiced by the loss of the ESI and whether Veeva acted with intent to deprive IQVIA of the information's use in the litigation. The Special Master finds that IQVIA has demonstrated that it is prejudiced by the deletion of EUStage. Courts have found prejudice exists where documents that are relevant to a claim are unavailable and the moving party has come forward with a plausible, good faith suggestion as to what the evidence might have been. *See GN Netcom, Inc.*, 2016 WL 3792833, at *6; *Schmid*, 13 F.3d at 80. *See also* Fed. R. Civ. P. 37(e)(1) Advisory Committee Notes 2015 ("An evaluation of prejudice from the loss of information necessarily includes an evaluation of the information's importance in the litigation."). IQVIA has come forward with a plausible, good faith suggestion as to what the audit trail would have shown, but for the deletion of EUStage. The deleted ESI bears directly on IQVIA's ability to prove its claims and defenses.

IQVIA asks the Special Master to enter default judgment as to Veeva's liability on IQVIA's claims and dismiss Veeva's counterclaims, sanctions the Special Master can recommend only upon a finding that Veeva intended to deprive IQVIA of the evidence. The Special Master is troubled by Veeva's conduct, it finds that IQVIA has met its burden to show that Veeva acted with intent to deprive it of the evidence. There is strong suspicion as to the

timing of the deletion of EUStage, marking it for deletion three days after Veeva provided its June 1, 2018, response indicating that it had no audit log that would show that Veeva performed data copying. Moreover, under the ESI Order, Veeva was clearly obligated to preserve EUStage. The Special Master finds this circumstantial evidence to be a sufficient basis on which to find that Veeva acted with the intent to spoliate relevant evidence.

Having found that IQVIA is prejudiced pursuant to Rule 37(e)(1) and finding that Veeva had the requisite intent pursuant to Rule 37(e)(2), the Special Master considers which sanctions to impose. Sanctions available under Rule 37(e)(2) include: (1) presuming that the lost information was unfavorable to Veeva; (2) instructing the jury that it may or must presume the information was unfavorable to Veeva; or (3) dismissing the action or entering a default judgment. In determining the appropriate sanction the Special Master considers the "(1) the degree of fault of the party who altered or destroyed the evidence; (2) the degree of prejudice suffered by the opposing party; and (3) whether there is a lesser sanction that will avoid substantial unfairness to the opposing party and, where the offending party is seriously at fault, will serve to deter such conduct by others in the future." *GN Netcom, Inc.*, 930 F.3d at 82 (quoting *Schmid*, 13 F.3d at 79).

The Special Master finds that IQVIA has sufficiently demonstrated that the deleted audit trails contained in EUStage would likely have been central evidence utilized at trial. To cure the prejudice suffered by IQVIA, the Special Master recommends that the District Court allow IQVIA to present evidence to the jury regarding the loss of evidence and to issue an adverse inference jury instruction that it deems fit to assist in the jury's evaluation of such evidence. The Special Master finds that such a sanction is appropriate because it cures the prejudice to IQVIA, but is no more severe than necessary. The Special Master believes that an adverse jury

instruction is appropriate in this instance both to punish Veeva and to deter such conduct by others in the future. The Special Master does not believe default judgment is the appropriate sanction in this instance. While the Special Master believes that the deletion of EUStage has prejudiced IQVIA and that Veeva acted with the requisite intent, an adverse jury instruction is an effective alternative to dismissal because it will allow IQVIA to present evidence to the jury and allow the jury to infer that the evidence contained in EUStage would have been unfavorable to Veeva. Dismissal is a drastic sanction that strikes at the heart of a lawsuit. *See Mosaid Techs. Inc.*, 348 F. Supp. 2d at 335. Because an adverse jury instruction will cure the prejudice to IQVIA, the Special Master believes it is the more appropriate sanction.

D. Google Drive

The elements of spoliation are first, "the spoliating party was under a duty to preserve when the loss occurred," second, "the lost ESI was within the scope of the duty to preserve," third, "the information was lost because the party failed to take reasonable steps to preserve" it, and fourth, "because ESI 'often exists in multiple locations,' spoliation occurs only where the information is truly lost and not recoverable elsewhere." *Bistrian*, 448 F. Supp. 3d at 465 (quoting Fed. R. Civ. P. 37(e) Advisory Committee's Note to 2015 Amendment).

As explained below, the Special Master finds that IQVIA has not met its burden to demonstrate that spoliation occurred with respect to Google Drive. There is no dispute that Veeva had a duty to institute a litigation hold to preserve potentially relevant ESI as of the date IQVIA filed suit. Veeva explains that it believed its subscription to Google Vault in January 2017 resulted in the preservation of documents on Google Drive. However, Veeva later learned that its preservation efforts did not extend to Google Drive and thus, the preservation functionality was not instituted until April 2017. IQVIA argues that Veeva employees were

therefore free to delete documents from Google Drive until April 2017. However, IQVIA fails to point to any documents with any reasonable particularity that were deleted from Google Drive as a result of Veeva's failure to institute a litigation hold. IQVIA mentions documents referenced in the depositions of Johnston, which could not be located by Veeva, but IQVIA has not explained what these documents were or their relevance to the lawsuit.

Even assuming that documents were deleted as the result of Veeva's delay in issuing a litigation hold on Google Drive, the Special Master is unable to issue sanctions pursuant to Rule 37(e)(1) and (e)(2). First, to find that sanctions are warranted pursuant to Rule 37(e)(1) the Special Master must find that IQVIA was prejudiced by the deletion of ESI. "Prejudice to opposing parties requires a showing [that] the spoliation 'materially affect[ed] the substantial rights of the adverse party and is prejudicial to the presentation of his case.'" *Magnetar Techs. Corp. v. Six Flags Theme Park Inc.*, 886 F. Supp. 2d 466, 481 (D. Del. 2012) (quoting *Micron Tech., Inc. v. Rambus Inc.*, 645 F.3d 1311, 1328 (Fed. Cir. 2011)). The moving party must offer "plausible, concrete suggestions as to what [the lost] evidence might have been." *GN Netcom, Inc.*, 930 F.3d at 83 (citing *Schmid*, 13 F.3d at 79). When the moving party cannot or does not, "there should be no finding of prejudice." *Id.*

Here, other than referring to documents it became aware of during the deposition of Johnston, IQVIA has not provided any information related to what documents may have been deleted from Google Drive and how such documents were relevant to its claims and defenses in this matter. There has simply not been any suggestion as to what the lost evidence would have revealed. IQVIA merely argues that because the Google Vault function was not applied to Google Drive documents until April 2017, Veeva employees could have deleted documents from Google Drive. The Special Master cannot find prejudice based on this assertion alone.

Second, there is no evidence in the record to support that Veeva affirmatively deleted documents from Google Drive during this time period. Thus, intent is lacking pursuant to Rule 37(e)(2). While the failure to institute a litigation hold in pending litigation may constitute gross negligence and sufficient culpable conduct to warrant sanctions, *see State National Insurance Co. v. City of Camden*, No. CV 08-5128 (NLH/AMD), 2011 WL 13257149, at *5 (D.N.J. June 30, 2011) (citing *Crown Castle USA*, 2010 WL 1286366 (W.D.N.Y. Mar. 31, 2010) at *11), negligent or even grossly negligent behavior does not logically support an adverse inference as the information lost through negligence may have been favorable to either party, including the party that lost it. *See* Fed. R. Civ. P. 37(e), Advisory Committee Note to 2015 Amendment. "Subsection (e)(1) is thus concerned with a party's negligent or grossly negligent failure to preserve ESI, whereas subsection (e)(2) is directed to instances where a party intentionally destroyed or lost ESI." *CIGNEX Datamatics, Inc. v. Lam Research Corp.*, No. CV 17-320 (MN), 2019 WL 1118099, at *2 (D. Del. Mar. 11, 2019); Fed. R. Civ. P. 37(e)(2) Advisory Committee Notes to 2015 Amendment ("The better rule for the negligent or grossly negligent loss of [ESI] is to preserve a broad range of measures to cure prejudice caused by its loss [i.e., (e)(1)], but to limit the most severe measures to instances of intentional loss or destruction [i.e., (e)(2)].").

While the Special Master does find that Veeva has provided contradictory statements to IQVIA as to when the Google Vault function was applied to Google Drive, IQVIA has not met its burden to demonstrate what evidence may have been lost as a result. Moreover, the Special Master finds the circumstantial evidence relied upon by IQVIA alone to be an insufficient basis on which to find that Veeva acted with the intent to spoliate relevant evidence. However, in light of Veeva's contradictory statements and the importance of when the litigation hold was applied to Google Drive, the Special Master will order Veeva to produce the full Google Vault report as

to Google Drive pursuant to the Court's inherent powers to manage discovery. Should that report reveal any deleted documents or disparities as to when the Google Vault functionality was applied to Google Drive, IQVIA may raise that issue with the Special Master. The Special Master otherwise declines to sanction Veeva pursuant to Rule 37(e) for its delay in issuing a litigation hold for documents contained on Google Drive.

E. James Kahan E-mails

As previously discussed, the Special Master has determined that Veeva's obligation to preserve documents in anticipation of litigation began in September 2015. Once a party reasonably anticipates or knows of pending litigation and the duty to preserve has attached, a party "must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents." *Sanofi-Aventis Deutschland GmbH*, 2010 WL 2652412, at *3 (citations omitted). Accordingly, by September 2015, Veeva should have suspended any Kahan e-mail deletions whether due to storage limitations or other reasons.

The Special Master first determines whether evidence was lost as a result of Veeva's failure to preserve Kahan's e-mails when its preservation obligation arose in September 2015. Veeva does not contest that Kahan's e-mails from January 2014 through May 2015 are missing. IQVIA has also demonstrated that Kahan's e-mails were deleted sometime after September 23, 2015, because Kahan was able to go back through e-mails from that time period as of that date. However, Veeva asserts that spoliation has not occurred because it produced 6,800 of Kahan's e-mails from that 17-month period that were in the possession of other custodians.

The Special Master believes that given the extended period of time (17 months) in which potentially relevant e-mails were lost, it is more probable than not that the failure to preserve the

same effects substantial prejudice. *See Diocese of Harrisburg v. Summix Dev. Co.*, No. 1:07-CV-2283, 2010 WL 2034699, at *1 (M.D. Pa. May 18, 2010). IQVIA explains Kahan's relevance to this matter, as he was extensively involved in the establishment and growth of Veeva OpenData, which IQVIA alleges Veeva misappropriated from IQVIA's Reference Data. IQVIA has also pointed to e-mails in the possession of other custodians, which Kahan drafted at this time that demonstrate examples of Veeva's alleged theft. These include a June 3, 2014, e-mail written by Kahan that states: "We use the results of the data report cards to identify any potential gaps in the Veeva reference data and pro-actively have our data stewardship team do the research and work to fill those gaps well before a client goes live." IQVIA also points to an April 25, 2014, e-mail to Johnston and Bill Henley wherein Kahan asks whether either has "BI's data that we received for a report card somewhere?" As such, the Special Master believes IQVIA has "come forward with plausible, concrete suggestions as to what that evidence might have been[,]" *Schmid*, 13 F.3d at 80.

In light of the fact that Kahan was extensively involved in Veeva's OpenData and that e-mails from a 17-month period were deleted, the Special Master believes it was more likely than not that potentially relevant e-mails were lost. While Veeva produced 6,800 Kahan e-mails from other custodians, there is no dispute that Kahan e-mails which were not sent from or received by custodians from this period have been lost.

Next, the Special Master must determine whether Veeva had the requisite intent to destroy ESI pursuant to Rule 37(e)(2). When ESI is lost, but a plausible, good faith explanation is given as to how the evidence became unavailable, Rule 37(e)(1) sanctions are appropriate. *See Folino v. Hines*, No. CV 17-1584, 2018 WL 5982448, at *3 (W.D. Pa. Nov. 14, 2018); *Sinclair v. Cambria Cty.*, No. 17-149, 2018 WL 468911, at *2–3 (W.D. Pa. Sept. 28, 2018) (awarding

sanctions of costs and fees under Rule 37(e)(1) where relevant text messages were allegedly deleted automatically and by mistake). If, however, a party acts in bad faith with intent to conceal the evidence from its opponent, the harshest sanctions under Rule 37(e)(2) are available. *See Folino*, 2018 WL 5982448, at *3*; Goldrich*, 2018 WL 4489674 at *1–2 (finding intent to deprive and imposing sanctions under Rule 37(e)(2) where plaintiff stated a "virus" made information unavailable, but forensic examination showed he gave opponent a computer with no data that was not even used during the relevant time frame); *see also Bull*, 665 F.3d at 79 (A "finding of bad faith is pivotal to a spoliation determination."). A finding of intent to deprive may be based on circumstantial evidence. *Goldrich*, 2018 WL 4489674, at *2.

The Special Master is persuaded that IQVIA has met its burden to demonstrate intent. The e-mails were still available in September 2015 when Veeva's duty to preserve arose. Only an intentional action could have resulted in the deletion of the e-mails. While Veeva suggests that Kahan's e-mails may have innocently been deleted due to storage constraints, Kahan confirmed that while he had deleted e-mails in the past, he had no personal knowledge when, how, or why all of his e-mails over this 17-month period were deleted. The testimony illustrates that Kahan's e-mails were not subject to automatic deletion, but rather someone would have to purposefully go in and delete them. The Special Master further notes that it is highly suspicious that no one at Veeva is able to confirm when, how, or why Kahan's e-mails were deleted. Veeva was acutely aware of the importance of Kahan's e-mails from this time period given Kahan's role in developing OpenData. The apparent failure to issue a litigation hold to suspend any deletion of his e-mails for this critical time period when its duty to preserve arose in September 2015 is troubling.

Having found that IQVIA had the requisite intent pursuant to Rule 37(e)(2), the Special Master considers which sanctions to impose. When considering which sanctions to impose under Rule 37(e)(2), the following factors act as a guide: "(1) the degree of fault of the party who altered or destroyed the evidence; (2) the degree of prejudice suffered by the opposing party; and (3) whether there is a lesser sanction that will avoid substantial unfairness to the opposing party and, where the offending party is seriously at fault, will serve to deter such conduct by others in the future." *Schmid*, 13 F.3d at 79. After weighing these factors, it is the Special Master's determination that the prejudice suffered by IQVIA and the degree of fault attributable to Veeva warrants an adverse jury instruction inference. First, the Special Master believes the degree of fault is high. A strong degree of fault exists where "there has been actual suppression or withholding of evidence." *Brewer v. Quaker State Oil Refining Corp.*, 72 F.3d 326, 334 (3d Cir. 1995). As discussed above, Veeva was in control of Kahan's e-mails, the deletion of the e-mails was intentionally performed, and the deletion occurred after Veeva anticipated litigation. Second, the prejudice to IQVIA is also very high. Not only has IQVIA been deprived of the audit trails from EUStage, but it has also been deprived of Kahan's contemporaneous e-mails. The Special Master declines, however, to recommend the harshest sanction of default judgment. While IQVIA has been deprived of critical evidence, the Special Master believes an adverse jury instruction is sufficient to cure the prejudice to IQVIA, punish Veeva for its actions and appropriately deter. *See Edelson v. Cheung*, No. 13-5870, 2017 WL 150241, at *4 (D.N.J. Jan. 12, 2017) (declining to impose default judgment, and instead sanctioning defendant with a jury instruction, where the defendant destroyed e-mails but there was additional evidence in the record which could prove plaintiff's allegations).

The Special Master recommends that the District Court allow IQVIA to present evidence to the jury regarding the loss of the Kahan e-mails and to issue an adverse inference jury instruction that it deems fit to assist in the jury's evaluation of such evidence. The Special Master finds that such a sanction is appropriate because it cures the prejudice to IQVIA, but is no more severe than necessary. Additionally, the Special Master will order Veeva to produce the full Google Vault Report related to Kahan's e-mails so that IQVIA may ascertain precisely when a litigation hold was applied to Kahan's e-mails and determine whether any e-mails were deleted after the litigation hold was applied.

Fraud Motion

I. Introduction

IQVIA believes that Veeva misused its data that it obtained through the DRC process. The DRC process is a marketing tool Veeva used; Veeva offered to compare data in use by a potential customer to Veeva's competitive OpenData offering. IQVIA believes that through this process, Veeva obtained IQVIA data from IQVIA customers and misused it to improve Veeva's OpenData product. IQVIA argues that evidence shows that not only did Veeva conduct these unauthorized analyses of IQVIA data in the first place, but Veeva then exploited its access to IQVIA's data well after any given DRC was completed, by, for example, improperly using IQVIA's data to identify and fill gaps in Veeva's competitive OpenData offering

In July 2018, Veeva served supplemental responses to interrogatories identifying seventy-four times when it extracted data from life sciences companies, including performing DRCs. Then, in November 2018, IQVIA served Interrogatory No. 36, requesting information available to Veeva about the circumstances of the deletion of the IQVIA data that Veeva obtained during the DRC process. Veeva responded that it generally deleted the files at or around

the time the DRC was completed. In August 2019, IQVIA moved to compel a complete response to Interrogatory No. 36. Veeva represented that there was no additional information responsive to Interrogatory No. 36. IQVIA then withdrew its motion. On February 17, 2020, at the close of fact discovery, Veeva produced fifty-one JIRA tickets.[11] JIRA is used by companies like Veeva for issue tracking and project management. IQVIA argues that these JIRA tickets are responsive to Interrogatory No. 36 because they provide an approximation of when employees deleted DRC extracts. It believes Veeva lied to IQVIA and the Court by not producing them earlier.

On March 16, 2020, IQVIA filed a motion for discovery regarding Veeva's apparent fraud on the Court seeking: (1) a complete response to IQVIA Interrogatory No. 36; (2) production of all documents or records, including, without limitation, communications among and between Veeva employees and personnel (including but not limited to Veeva's in-house counsel), Veeva's outside counsel, Veeva's vendors, Veeva's experts, and/or any person acting on Veeva's behalf, relating to: (a) the preparation of Veeva's responses (including all supplemental responses) to IQVIA's first interrogatories relating to the deletion of data extracts; (b) the preparation of Veeva's response to Interrogatory No. 36; and (c) the preparation of Veeva's August 16, 2019, opposition to IQVIA's August 2, 2019, motion to compel, including the declarations submitted in support of that opposition; (3) production for deposition, of up to three hours each, persons with knowledge on the topics listed in (2) above, including the following individuals: (a) Josh Faddis; (b) Charles Tait Graves; (c) Veeva's outside counsel responsible for the Opposition, whether Arnold Calmann or otherwise; (d) Patrick Young; (e)

[11] In a November 30, 2018, Order, the Special Master ordered Veeva to produce certain Computer Forensic Discovery—including relevant portions of Veeva's JIRA trouble ticketing database. Veeva appealed that order and it remains pending before the District Judge. In light of its appeal, Veeva has refused to produce the relevant portions of the JIRA database.

Holly Stites; (f) Jonathan Johnston; and (g) Candice Iha. Veeva filed opposition to IQVIA's motion on May 14, 2020. Thereafter, IQVIA filed a reply brief on July 14, 2020.

However, IQVIA's reply to Veeva's opposition modified the relief it was seeking to a request that the Special Master order: (1) Veeva to respond to IQVIA's Interrogatory 36 in full, including by producing responsive information (including, but not limited to responsive JIRA tickets); (2) that the jury be informed that Veeva made false representations during discovery to hide evidence regarding Veeva's deletion of data extracts used to prepare DRCs; and (3) that Veeva is prohibited from presenting evidence or argument to the jury and to the Court that Veeva timely deleted data extracts used to prepare DRCs, pursuant to any policies, agreements, or otherwise. IQVIA further requests that the Special Master award IQVIA its reasonable expenses, including attorneys' fees, in connection with IQVIA's motion to compel a response to Interrogatory No. 36 and reply in support thereof, and IQVIA's present motion and reply.

II. Arguments of the Parties

A. IQVIA Arguments

IQVIA explains that its trade secret misappropriation claims against Veeva include Veeva's misuse of IQVIA's data that Veeva obtained through the DRC process. According to IQVIA, the evidence shows that, not only did Veeva conduct these unauthorized analyses of IQVIA data in the first place, but Veeva then exploited its access to IQVIA's data well after any given DRC was completed by improperly using IQVIA's data to identify and fill gaps in Veeva's competitive OpenData offering.

In the first set of interrogatories IQVIA served in September 2017, IQVIA requested that Veeva identify the data extracts that Veeva had received from life sciences companies, including its receipt of IQVIA's data. On July 2, 2018, Veeva served a supplemental response to IQVIA's

first interrogatories identifying seventy-four times when it extracted data from life sciences companies, including to perform a DRC. Veeva identified an additional fourteen DRCs in a supplemental response served on December 21, 2018.[12] For forty-eight of these instances, Veeva stated that "[a]ny such extract was deleted prior to the litigation" or that "Veeva believes [the extract] was deleted prior to the litigation."

In November 2018, IQVIA served Interrogatory No. 36 requesting information reasonably available to Veeva about the circumstances of deletion, including when the file was deleted, by whom, and how, and identify with specificity the basis for Veeva's belief that the file may have been deleted. IQVIA asserts that in response, Veeva vaguely referred to a "stated policy" of deleting extracts provided by potential customers for purposes of DRCs and its "understanding" that the extracts were "generally" deleted "at or around the time" a DRC was completed.[13]

On August 2, 2019, IQVIA moved to compel a complete response to Interrogatory No. 36. Veeva filed its Opposition on August 16, 2019, arguing that the information IQVIA sought did not exist. Veeva's Opposition was signed by Arnold Calmann, Veeva's then outside counsel. Veeva also submitted three declarations from its IT personnel: Patrick Young, Holly Stites, and Jonathan Johnston, which swore that "Veeva does not possess information that could show when a particular document was deleted" from various file storage repositories at Veeva (Google Drive and Google e-mail, Egnyte, FTP, NAS, and Hightail) based on their investigations. On August 23, 2019, IQVIA withdrew its motion as moot.

[12] Veeva's General Counsel Josh Faddis signed the formal verification under Rule 33(b)(5) for these interrogatory responses, and the responses were also signed by Veeva's outside counsel Charles Tait Graves.

[13] Veeva's response to Interrogatory No. 36 was again formally verified by Mr. Faddis under Rule 33(b)(5) and signed by Veeva's outside counsel, Mr. Graves.

On February 17, 2020, Veeva produced fifty-one tickets from JIRA. IQVIA believes the JIRA tickets contain some of the very information that IQVIA requested in Interrogatory No. 36 and that Veeva swore did not exist. By way of illustration, IQVIA points to Veeva's supplemental responses to IQVIA's first interrogatories, wherein Veeva stated that it had received a data extract from a life sciences company named Grifols; that it "believes the data extract was saved to a shared network space in Veeva's Egnyte file repository"; and that "[a]ny such extract was deleted prior to the litigation." IQVIA argues that despite the specificity of Veeva's representation—that the Grifols extract was deleted prior to the litigation, Veeva denied that it had any further information about when, by whom, and how that extract was deleted. However, Veeva's production of the JIRA tickets shows that Veeva received a data extract from Grifols for the purpose of preparing a DRC; the data extract from Grifols was "located on Egnyte"; and that it was "purged" by Veeva employee Eric Davis on October 13, 2016, after Veeva's duty to preserve had arisen. IQVIA argues that this information concerning the deletion of the Grifols data extract was precisely the type of information that Veeva repeatedly represented did not exist.

The Grifols JIRA ticket was generated by Candice Iha, an employee of Veeva's discovery vendor Consilio, Inc., less than a week before Veeva served its July 2, 2018, supplemental responses to IQVIA's first interrogatories. From the date that this JIRA ticket was generated, IQVIA believes Veeva relied upon the JIRA ticket (and others like it) to formulate its supplemental responses to IQVIA's first interrogatories, but then when asked for the factual basis of its responses (in Interrogatory No. 36), Veeva *falsely* represented that no further information existed.

In its February 17, 2020, production, Veeva produced six other JIRA tickets that were generated by Veeva's discovery vendor days before Veeva served its supplemental interrogatory responses on July 2, 2018. IQVIA believes that Veeva is withholding other JIRA tickets that likely exist and contain information that Veeva falsely stated did not exist. IQVIA thus requests leave to take additional discovery to gain clarity into whether Veeva's false statements to the Court warrant the imposition of severe sanctions. IQVIA argues that Veeva's prior false statements deprived it of the ability to use this information to pursue its claims of trade secret theft and evidence spoliation during the fact discovery period.

IQVIA requests that Veeva now be compelled to respond fully to Interrogatory Number 36, and that Veeva be ordered to produce additional document discovery and deposition testimony focused on the extent to which Veeva and its counsel deliberately misled the Court and IQVIA. IQVIA relies on Rule 26(g), Rule 26(e), and Rule 37(c) for the relief sought. IQVIA further relies on the Special Master's inherent power to "manage its case docket, including making decisions of when and how to conduct discovery." *Vanderwerff v. Quincy Bioscience Holding Co., Inc.*, 2018 WL 6243040, at *4 (D.N.J. Nov. 28, 2018) (court has inherent "authority to fashion tools that aid the court in getting on with the business of deciding cases" (citation omitted)).

IQVIA argues that the relief it requests is necessary because Veeva's outright denial that any responsive information existed appears inexcusable, given that the eight JIRA tickets at issue were generated by Veeva's discovery vendor on June 22 and June 26, 2018—just days before Veeva served its July 2, 2018, supplemental responses to IQVIA's first interrogatories. IQVIA believes that these facts strongly suggest that Veeva affirmatively relied upon these eight JIRA

tickets in preparing its supplemental responses. IQVIA does not believe that Veeva's attorneys could have made a reasonable inquiry and still have missed the JIRA tickets.

IQVIA argues it was prejudiced by Veeva's false representations because it deprived IQVIA of the ability to take discovery related to the facts about the deletion of these data extracts that Veeva hid through its false statements. IQVIA asserts that Veeva is likely still hiding facts from other JIRA tickets that surely exist, but which Veeva did not include in its February 2020 production. IQVIA does not believe that Veeva would have included any JIRA tickets that would have shown it acting improperly by, for example, deleting data extracts only after litigation started.

IQVIA also asks the Court to order Veeva to produce for deposition all persons with knowledge of the "False Representation Discovery." IQVIA argues any privilege objection should be overruled on the basis of the crime-fraud exception. IQVIA asserts that the crime-fraud exception applies to documents and communications relating to Veeva's potential fraud on this Court. IQVIA argues that Veeva falsely represented to the Special Master and IQVIA that there was no information responsive to when and by whom the data extracts at issue were deleted.

B. Veeva's Opposition

Veeva asserts that it built up its data records for OpenData through a variety of ordinary, lawful means. Veeva explains that DRCs are a standard marketing tool used by data providers to try to show potential customers that a data product would give them better data. Veeva asserts that before it obtained the customer's extract, customers were required to confirm that they approved the DRC and had rights to the data they were providing. Veeva argues that at no point did customer data mix into Veeva's OpenData product. Veeva stored the customer extracts in file

storage systems that were outside of, and independent from, the OpenData master dataset. Those file storage systems were called Egnyte, FTP, NAS, Hightail, and Google e-mail/Google Drive.

Veeva explains that its standard, ordinary-course policy was to delete the extract that each customer made available for the DRC. Veeva argues there was nothing unexpected or untoward about such deletions. As Veeva reported in its interrogatory responses, in some cases Veeva employees missed copies of DRC extracts when deleting them, such as a copy in someone's e-mail Sent Items. Veeva maintains that it produced those leftover DRC extracts. Veeva believes its litigation hold also captured certain DRC extracts that might otherwise have been permanently deleted.

Veeva argues that it objected to Interrogatory No. 36 on scope and burden grounds. Relying on these objections, Veeva then explained that, based on its investigation – including its investigation of "contemporaneous e-mail" – DRC extracts were generally deleted "at or around the time" each project ended:

> The basis for Veeva's belief that such files were deleted in the ordinary course, beyond Veeva's oft-stated assertion that it would do so, is based on Veeva's investigation of whether such materials still existed at any of those types of locations in connection with document discovery in this case. Except where otherwise reported, Veeva found that the files no longer existed in those locations. (Where Veeva located any such file that still existed, Veeva produced it.) Veeva's understanding is that the employees who worked on the data comparison marketing exercises, who are listed in Veeva's interrogatory responses and reflected in Veeva's document productions, generally deleted such files at or around the time the marketing data comparison exercise was completed. Also, in many instances, contemporaneous e-mail reflected that Veeva employees working on the marketing data comparison exercises deleted the files from such locations.
>
> In no instance has Veeva uncovered any indication that any file described in any of Veeva's interrogatory responses was deleted for purposes of avoiding production in this litigation, or that any

> such file was deliberately or knowingly not preserved for purposes of potential discovery in this litigation.

Veeva also described the file storage systems where extract files were stored for purposes of the projects.

In opposition to IQVIA's August 2019 motion to compel, Veeva asserts that it referred back to its interrogatory response, describing how it had worked hard to determine if the five specific file storage tools where it had stored DRC extracts – Egnyte, FTP, NAS, Hightail, and Google e-mail/Google Drive – contained software logs or other recording mechanisms that could identify when, exactly, a user hit the delete button to delete a DRC extract. In support of its response, Veeva included three declarations from its IT personnel, who testified to specific characteristics of the five file storage systems. According to Veeva, each of these declarations clearly stated that the declarant was speaking as to the specific file storage systems. Each made the same point that none allowed any way to determine the exact date when an employee hit the delete button in each system. Veeva argues that it did not state that there was no information whatsoever that would point to the approximate timeframe someone deleted a DRC extract. Instead, Veeva's response to Interrogatory No. 36 pointed to less precise sources of information it had already produced, such as e-mails.

Veeva argues that JIRA is not a file storage system and is not a log of exact dates when files in storage systems such as Egnyte or FTP were deleted. It is a ticketing system where employees can post messages that others can respond to. Veeva argues that if one of its employees generated a JIRA ticket stating he or she has deleted a DRC extract, which is merely the employee's report of actions he or she carried out in other systems. According to Veeva, it does not demonstrate the exact moment when the employee hit the delete button, like a system time stamp would. At best, JIRA can provide clues as to the most likely date range when

employees deleted a data extract. By way of example, Veeva points to its Exhibit 14 – an October 2016 JIRA ticket concerning the deletion of a DRC extract for a customer called Grifols. The JIRA ticket features one employee reporting "Data Purged," two days after a colleague instructed him to make sure to delete the extract. Veeva argues that based on this, one cannot tell for certain if the employee deleted the extract the day of the message on the JIRA ticket, two days earlier, or at another time.

Veeva argues that its February 2020 production did not contain information of a type that IQVIA had never seen before. Veeva explains that its JIRA system creates contemporaneous e-mail records with the exact content from JIRA tickets, informing employees working on the tickets of updates to the ticket. Because many of the parties' agreed-upon custodians received such JIRA ticket updates by e-mail, Veeva produced tens of thousands of e-mails containing content from thousands of JIRA tickets. Veeva argues that IQVIA thus already had the information showing that Veeva employees used JIRA tickets to ask for and confirm deletion of DRC extracts.

Veeva further argues that its response to Interrogatory No. 36 and related briefing were accurate and consistent with the JIRA tickets it later produced. It believes IQVIA's motion offers nothing to contradict its assertion that DRC extracts were deleted by Veeva employees soon after each project was completed. Veeva argues that IQVIA's conjectures – that Veeva attorneys engaged in a conspiracy with a document collection vendor employee named Candice Iha to withhold information from JIRA tickets collected (among millions of other documents)– are incorrect and outlandish.

Veeva further argues that IQVIA fails to explain why deletions of DRC extracts are relevant to any specific claim of wrongdoing in this lawsuit. Veeva points out that from around

June 2016 forward, all of the customers who approved DRCs expressly confirmed to Veeva, in writing, that they were not providing data from IQVIA in the data extract. Moreover, Veeva argues that the one customer named in the JIRA tickets, Sunovion, had a TPA with IQVIA that authorized the data-matching work Sunovion hired Veeva to perform. Veeva also argues there is no reason it would have been obliged to preserve, and not delete, the very data extracts it told customers it would delete.

Veeva argues its response to Interrogatory No. 36 and subsequent briefing were "complete and correct as of the time [they were] made," Fed. R. Civ. P. 26(g)(1)(A); and they remain true today and do not require any supplementation. *See* Fed. R. Civ. P. 26(e)(1)(A) (describing when supplementation is required); Fed. R. Civ. P. 26(b)(1) (limiting overbroad discovery). Veeva argues that there is no requirement that a party responding to an interrogatory engage in "extensive research" to provide an answer. *See Legends Mgmt. Co., LLC v. Affiliated Ins. Co.*, No. 2:16-CV-01608 (SDW) (SCM), 2017 WL 4618817, at *3 (D.N.J. Oct. 13, 2017) (a responding party must make a reasonable effort, but is not required to "conduct extensive research to answer"; finding an interrogatory disproportionate in its entirety where a response would have no effect on the opponent's argument at trial) (citation omitted); *Reyes v. City of Paterson*, No. 2:16-CV-2627-ES-SCM, 2017 WL 1536425, at *2 (D.N.J. Apr. 28, 2017) (same); *Williams v. Acxiom Corp.*, No. 2:15-CV-08464-ES-SCM, 2017 WL 945017, at *2 (D.N.J. Mar. 10, 2017) (same); *see also Price v. Synapse Grp., Inc.*, No. 16-CV-1524 (BAS)(BLM), 2018 WL 9517276, at *7 (S.D. Cal. Sept. 12, 2018) ("[I]t would be unduly burdensome to require Defendants to interview every employee to determine whether that employee knows of potentially responsive ESI that Defendants would then be required to produce."); *Fischer & Porter Co. v. Sheffield Corp.*, 31 F.R.D. 534, 536 (D. Del. 1962) (holding that an interrogatory

requiring a party to investigate all of its employees for an eight-year period to discover if they had certain information was burdensome and oppressive). Veeva also argues that depositions of opposing counsel are strongly disfavored by courts throughout the country.

Veeva argues that it also reported accurately that based on employee e-mails and other factors, it believes that employees deleted the extracts "at or around the time" each project was completed. The JIRA tickets that Veeva produced in February 2020 do not alter these answers. Veeva also rejects any assertions of a conspiracy between lawyers and an employee of a document collection vendor. Veeva argues that it never claimed to have reviewed every single e-mail or JIRA ticket for purposes of responding to Interrogatory No. 36.

Veeva argues that its employee declarations were also truthful and accurate. Veeva maintains that it diligently had its employees who administer those systems – Hightail, FTP, Egnyte, Google e-mail/Google Drive, and NAS – search for any system logs or other electronic trails that would provide such information. The result was a determination that no such logs or trails exist. Thus, Veeva correctly reported that such information does not exist. Veeva again reiterates that JIRA tickets do not provide a time- and date-stamped record of exactly when someone hit the delete button in one or more of the five file storage systems. They were reporting the objective fact that specific file storage systems do not contain the date- and time-stamped information IQVIA sought.

Veeva argues that IQVIA's assertions that it attempted to conceal information is demonstrably false. Veeva asserts that it produced tens of thousands of JIRA-generated e-mails searchable by "JIRA" in the subject line. It argues that hundreds of these documents pertain to DRCs. Veeva argues that even if one were to assume that Veeva's attorneys wanted to commit a fraud, that does not explain why they would withhold information from a smattering of JIRA

tickets while producing tens of thousands of other JIRA-related documents, many of which resemble or match those very tickets.

C. IQVIA's Reply

IQVIA requests that in light of Veeva's Opposition, the Special Master consider Veeva's discovery misconduct as further evidence of Veeva's bad faith in connection with IQVIA's Sanctions Motion. In this respect, to the extent the Court does not impose the case-terminating sanctions requested in IQVIA's Sanctions Motion, IQVIA requests that the Special Master order: (1) Veeva to respond to IQVIA's Interrogatory No. 36 in full, including by producing responsive information (including, but not limited to responsive JIRA tickets); (2) that the jury be informed that Veeva made false representations during discovery to hide evidence regarding Veeva's deletion of data extracts used to prepare DRCs; and (3) that Veeva be prohibited from presenting evidence or argument to the jury and to the Court that Veeva timely deleted data extracts used to prepare DRCs, pursuant to any policies, agreements, or otherwise. IQVIA further requests that the Special Master award IQVIA its reasonable expenses, including attorneys' fees, in connection with IQVIA's Motion to Compel a response to Interrogatory No. 36 and Reply in support thereof, and IQVIA's present Fraud Motion and Reply.

IQVIA argues that any DRCs Veeva ran involving its Reference Data were unauthorized because IQVIA's licenses with customers did not allow Veeva to use IQVIA's data for these types of analyses. IQVIA further asserts that in addition to misappropriating IQVIA's Reference Data to prepare DRCs, Veeva also reused its Reference Data to fill in gaps in Veeva's OpenData product. IQVIA points to a June 2014 e-mail wherein a Veeva employee stated that Veeva "use[s] the results of the data report cards to identify any potential gaps in the Veeva Reference data and pro- actively have our data stewardship team do the research and work to fill those

gaps." Thus, IQVIA argues there is evidence that Veeva held onto data extracts for months after the DRCs were complete and improperly used them to update Veeva OpenData.

IQVIA argues that the circumstances of Veeva's deletions of data extracts are highly relevant. First, IQVIA explains that it seeks discovery into how long Veeva maintained its Reference Data, which it obtained while preparing DRCs. IQVIA believes the longer Veeva held onto the data, the more opportunity it had to misappropriate its Reference Data to improve Veeva's competing offerings. IQVIA argues that Veeva's claims that the extracts were timely deleted per policy is demonstratively untrue because Veeva still has dozens of them and Veeva admitted that its efforts to delete DRC extracts was not always perfect. Second, IQVIA seeks discovery into how long Veeva maintained its Reference Data to test the credibility of Veeva's assurances that it safeguarded the data extracts. Third, IQVIA asserts that when Veeva deleted the Reference Data is relevant because Veeva's duty to preserve arose no later than the fall of 2015. Thus, if Veeva deleted relevant data extracts after its duty to preserve had arisen, IQVIA believes this is further evidence of spoliation that supports IQVIA's Sanctions Motion.

IQVIA rejects Veeva's argument that JIRA tickets are not responsive to Interrogatory No. 36. IQVIA points out that Interrogatory No. 36 does not references "forensic timestamps." Instead, IQVIA asserts that it clearly requests information about the circumstances of deletion, a fact Veeva characterizes as the "fulcrum" of IQVIA's request.

IQVIA further argues that notwithstanding Veeva's representations throughout its opposition that it produced "thousands" of "JIRA tickets in an e-mail format," Veeva identifies only a handful of e-mails that relate to the deletion of data extracts. Moreover, the e-mails do not contain all the information available from the JIRA tickets. The e-mails do not show when the data extracts were deleted—information directly responsive to IQVIA's Interrogatory No. 36. By

way of example, IQVIA points to the Grifols auto-generated e-mail and the Grifols JIRA Ticket. The auto-generated e-mail shows only that, as of the date of the e-mail, a Veeva employee had requested that the data extract used to prepare the Grifols DRC be deleted. Meanwhile, the JIRA ticket reveals that the data extract was deleted as of October 13, 2016, provides a "description" of the data extract; the source of the extract (Grifols); purpose of the extract ("performing a standard DIR"); where the data extract was saved ("Egnyte"); and who approved the use of the data extract to prepare a DRC (Rebecca Silver).

IQVIA reiterates that the prejudice to it is apparent—as a result of Veeva's false statements about the absence of information in its possession showing when data extracts were deleted, IQVIA was unable to pursue that issue in discovery. It contends that re-opening potentially dozens of depositions is, at this juncture, impractical.

IQVIA argues that as an initial matter, Veeva should be ordered to fully respond to IQVIA's Interrogatory No. 36, including by producing responsive information. Veeva's current response to Interrogatory No. 36 is that the data extracts were "generally" deleted "at or around the time" each DRC was completed. IQVIA argues that this vague response does not provide any substantive information about the circumstances of deletion of any of the forty-eight deleted data extracts. IQVIA argues that instead of generically representing that the extracts were deleted "at or around the time" the DRCs were completed (with no further information, including date), far more precise responses would have been that Veeva deleted the extract it received from: Grifols at or around October 13, 2016, confirmed by Veeva employee Eric Davis; Sunovion at or around August 2, 2016, confirmed by Davis; Thermo Fisher at or around August 29, 2016, confirmed by Davis; Survey Health Care at or around October 13, 2016, confirmed by Davis; AAA Pharmaceutical at or around May 4, 2017, confirmed by Veeva employee Zak Rudzitskiy;

Optinose at or around May 22, 2017, confirmed by Veeva employee Jason Hill; Health Media Network at or around May 30, 2017, confirmed by Hill; and Sage at or around October 10, 2017, confirmed by Rudzitskiy. Although IQVIA now knows this information for eight of the forty-eight deleted data extracts, Veeva is continuing to withhold other information, including but not limited to JIRA tickets, showing (among other things) when the other forty such data extracts were deleted.

With respect to sanctions, IQVIA requests that Veeva's discovery misconduct be considered as evidence of bad faith in connection with IQVIA's Sanctions Motion. It further argues that the Court should instruct the jury that Veeva made false representations during discovery to hide evidence. IQVIA also believes the Court should prohibit Veeva from introducing evidence of its purportedly "timely" deletion of the data extracts. IQVIA also argues that the Court should award it reasonable expenses pursuant to Rule 37(c).

D. Veeva's Sur Reply

Veeva argues that IQVIA's request for sanctions based on the production of JIRA tickets, lodged for the first time in IQVIA's reply, should be denied for two reasons. First, Veeva argues it committed no fraud and made no false representation. Veeva truthfully confirmed that IQVIA's requested "metadata or software logs" containing precise deletion dates of DRC extracts do not exist. Veeva argues that IQVIA cannot show any intentional deceit or misrepresentation. Second, Veeva argues its discovery responses were more than adequate. Veeva reiterates that it diligently investigated IQVIA's questions regarding DRC extract deletions and reported the facts. Veeva accurately explained that it deleted DRC extracts "at or around the time" Veeva completed each DRC. No more was required.

Veeva asserts that its statements were true. With respect to IQVIA's request for "metadata or software logs" shedding further light on Veeva's DRC extract deletions, no such

information exists. IQVIA has not shown otherwise. Instead, Veeva argues that IQVIA distorted its response into a generalized claim that it possesses no information on DRC extract deletions. Veeva argues that it never said it lacked any information regarding the circumstances of DRC extract deletions. It stated only that it lacked the "exact date[s]" on which Veeva employees "hit the delete button." Veeva argues that compiling a list of deletion dates for DRC extracts would have been colossally burdensome and disproportionate.

III. Applicable Law

IQVIA's motion relies on Rule 26(g), which provides that an interrogatory response must be certified by an attorney of record as "complete and correct as of the time it is made." IQVIA also relies on Rule 26(e) which provides that a party "must supplement or correct" an interrogatory response "in a timely manner if the party learns that in some material respect the disclosure or response is incomplete or incorrect." To the extent a party fails to do so, the court may impose appropriate sanctions pursuant to Rule 37(c).

A. Rule 26(g)

"Rule 26(g) requires all attorneys to engage in pretrial discovery in a responsible manner consistent with the spirit and purposes of liberal discovery." *Younes v. 7-Eleven, Inc.*, 312 F.R.D. 692, 703 (D.N.J. 2015) (citing *Kosher Sports, Inc. v. Queens Ballpark Co., LLC*, No. 10–cv–2618 (JBW), 2011 WL 3471508, at *7 (E.D.N.Y. Aug. 5, 2011)(quoting Fed. R. Civ. P. 26(g) Advisory Committee Note to 1983 Amendment) (hereinafter "1983 Note")). Under Rule 26(g), "an attorney's signature certifies that any disclosures were complete and accurate at the time they were made and that a reasonable inquiry was made." *Younes*, 312 F.R.D. at 703 (citing *Singer v. Covista, Inc.*, C.A. No. 10–6147 (JLL), 2013 WL 1314593, at *9 (D.N.J. March 28, 2013)). "An objective standard is used to determine if a certification is reasonable." *Ibid.* (citing *St. Paul*

Reinsurance Company, Ltd. v. Commercial Financial Corp., 198 F.R.D. 508, 516 (N.D. Iowa 2000) ("The standard for imposing Rule 26(g) sanctions is objective.")).

"Rule 26(g) is cast in mandatory terms." *Younes*, 312 F.R.D. at 704 (D.N.J. 2015) (citing *Chambers v. NASCO, Inc.*, 501 U.S. 32, 51 (1991)). "Unless the offending conduct is harmless, a violation of Rule 26(g) without substantial justification must result in the imposition of sanctions." *Younes*, 312 F.R.D. at 703 (citing *Chambers*, 501 U.S. at 51). "Substantial justification exists where there is a genuine dispute or if reasonable people could differ." *Younes*, 312 F.R.D. at 703 (citing *Heller v. City of Dallas*, 303 F.R.D. 466, 477 (N.D.Tx.2014)).

It is left to the court's discretion to determine what Rule 26(g) sanction is appropriate. The Rule merely provides that the sanction be "appropriate." *Younes*, 312 F.R.D. at 704 (citing *Chambers*, 501 U.S. at 51). The sanction may be imposed against the certifying attorney, the client, or both. *Younes*, 312 F.R.D. at 704 (citing *Markey v. Lapolla Industries, Inc.*, No. CV 12–4622 (JS) (AKT), 2015 WL 5027522, at *18 (E.D.N.Y. Aug. 25, 2015)).

"Rule 26(g) does not require perfection and does not impose an unreasonably high burden on litigants. It simply requires that a reasonable inquiry be made into the factual basis of a discovery response and that responses to discovery be complete and correct when made." *Younes*, 312 F.R.D. at 706. "An attorney makes a 'reasonable inquiry' under Rule 26(g) if the investigation undertaken by the attorney and the conclusions drawn therefrom are reasonable under the circumstances." *Younes*, 312 F.R.D. at 707. "Ultimately, what is reasonable is a matter for the Court to decide on the totality of the circumstances." *Id.* at 707 (citing *Markey v. Lapolla Industries, Inc.*, No. CV 12–4622 (JS)(AKT), 2015 WL 5027522, at *15 (E.D.N.Y. Aug. 25, 2015) (citation and quotation omitted)). An objective standard is applied in determining whether sanctions are to be applied under Rule 26(g). *Younes*, 312 F.R.D. at 707 (citing *Grider v.*

Keystone Health Plan Central, Inc., 580 F.3d 119, 140 n. 23 (3d Cir. 2009) (citation and quotation omitted)).

B. Rules 26(e) and 37(c)

Rule 26(e) provides that a party who has responded to an interrogatory or request for production must supplement or correct its response if that party learns that in some material respect the response is incomplete or incorrect, and if the additional or corrective information has not otherwise been made known to the other parties during the discovery process or in writing. *See* Rule 26(e)(1)(A). Rule 26(e) thus imposes a duty to supplement responses to discovery requests throughout the litigation. *710 Bowers v. Nat'l Collegiate Athletic Ass'n.*, 475 F.3d 524, 538 (3d Cir.2007), amended on reh'g (March 7, 2007).

Rule 37(c) then provides that if a party fails to provide information as required by Rule 26(e), that party is not allowed to use that information at trial, unless the failure was substantially justified or is harmless. Fed. R. Civ. P. 37(c)(1). In addition to or instead of this sanction, the court: (A) may order payment of the reasonable expenses, including attorney's fees, caused by the failure; (B) may inform the jury of the party's failure; and (C) may impose other appropriate sanctions, including any of the orders listed in Rule 37(b)(2)(A)(i)-(vi). Fed. R. Civ. P. 37(c)(1). Rule 37 is written in mandatory terms and is designed to provide a strong inducement for disclosure. *See Horizon Blue Cross Blue Shield of New Jersey v. Transitions Recovery Program*, Civ. A. No. 10-3197, 2015 WL 1137777, at *3 (D.N.J. Mar. 13, 2015) (quoting *Newman v. GHS Osteopathic, Inc.*, 60 F.3d 153, 156 (3d Cir. 1995)).

In determining whether to impose sanctions pursuant to Rule 37(c)(1), the court should consider: "(1) prejudice or surprise to the [opposing party]; (2) the ability of [the opposing party] to cure the prejudice; (3) the likelihood of disruption; and (4) the [non-disclosing party's] bad faith or unwillingness to comply." *Wachtel v. Health Net, Inc.*, 239 F.R.D. 81, 104-05 (D.N.J.

2006) (citing *Newman v. GHS Osteopathic, Inc.*, 60 F.3d 153, 156 (3d Cir. 1995)). A fifth factor for consideration is "the importance of the excluded evidence." *Accurso v. Infra-Red Servs., Inc.*, 169 F. Supp. 3d 612, 616 (E.D. Pa. 2016) (citing *ZF Meritor, LLC v. Eaton Corp.*, 696 F.3d 254, 298 (3d Cir. 2012)).

C. The Court's Inherent Power

IQVIA also asserts that "the Court has 'inherent power to manage its caseload, control its docket, and regulate the conduct of attorneys before it,' which 'provides authority to fashion tools that aid the court in getting on with the business of deciding cases.'" *Vanderwerff v. Quincy Bioscience Holding Co., Inc.*, No. CV170784ESMAH, 2018 WL 6243040, at *4 (D.N.J. Nov. 28, 2018) (citing *Eash v. Riggins Trucking Inc.*, 757 F.2d 557, 567 (3d Cir. 1985)); *see also Landis v. N. Am. Co.*, 299 U.S. 248, 254, 57 S. Ct. 163, 165, 81 L. Ed. 153 (1936) (recognizing the "the power inherent in every court to control the disposition of the causes on its docket with economy of time and effort for itself, for counsel, and for litigants"); *United States v. Wecht*, 484 F.3d 194, 217 (3d Cir. 2007) ("It is important to note that district courts have wide discretion in the management of their cases.").

IV. Opinion

The Special Master finds that the JIRA tickets produced by Veeva on February 17, 2020, do contain information responsive to Interrogatory No. 36. Further, the Special Master finds that the JIRA tickets do contain information that was not previously provided to IQVIA, in JIRA e-mail format or otherwise. The JIRA tickets may not indicate the exact date or time a data extract was deleted, but they certainly constitute evidence about the circumstances of deletion and provide evidence as to the dates the data extracts were deleted. Next, the Special Master will evaluate whether failure to provide these JIRA tickets in response to Interrogatory No. 36 or after IQVIA filed its motion to compel violated Rule 26(g) or Rule 26(e).

Under Rule 26(g) an attorney's signature certifies that any response was complete and accurate at the time it was made and that a reasonable inquiry was made. *See Younes*, 312 F.R.D. at 703. According to the record, Veeva's vendor generated the JIRA tickets at issue in June 2018, just before Veeva served its July 2, 2018, response to IQVIA's First Set of Interrogatories. Then, in November 2018, IQVIA served Interrogatory No. 36, which stated:

> For each instance in Veeva Systems Inc.'s Objections and Second Supplemental Responses to IMS's First Set of Interrogatories (Nos. 1-15), dated July 2, 2018, where Veeva stated that it believed that certain files discussed in the responses were, or may have been, "deleted prior to the litigation," provide all information reasonably available to Veeva about the circumstances of deletion, including when the file was deleted, by whom, and how, and identify with specificity the basis for Veeva's belief that the file may have been deleted.

A fair reading of Interrogatory No. 36 indicates that IQVIA was seeking reasonably available information about the circumstances of deletion, not just a system log or other electronic trail that would provide the exact date a file was deleted. Veeva responded to Interrogatory No. 36 on December 21, 2018. In its response, Veeva indicated that the data extract files discussed in Veeva's July 2, 2018, and prior interrogatory responses were generally stored in 4 types of locations: FTP servers, a Network Attached Storage (NAS) device, Veeva's Egnyte file storage system, or a cloud storage system such as Google Drive. Veeva then indicated that the basis for its belief that such files were deleted in the ordinary course was based on Veeva's investigation of whether such materials still existed at any of those types of locations in connection with document discovery in this case. Veeva then explained that except where otherwise reported, it found that the files no longer existed in those locations. Veeva did not mention and did not serve any JIRA tickets in response to Interrogatory No. 36.

IQVIA then filed a motion in August 2019 which sought to have the Court order Veeva to provide a complete response to Interrogatory No. 36 by providing all information reasonably available to Veeva about the circumstances of deletion of the extracts—when each extract was deleted, by whom, how the deletion occurred (including whether it was pursuant to direction by a Veeva employee and if so, who; pursuant to a Veeva policy and, if so what policy; and the method used to execute the deletion), and the basis for Veeva's belief that the file(s) may have been deleted. Veeva's August 19, 2019, Opposition clearly indicted that "Interrogatory 36 demands information Veeva does not believe exists after reasonable investigation, and that Veeva therefore cannot provide." Accordingly, IQVIA withdrew its motion.

The Special Master does not find that Rule 26(g) was violated when Veeva provided its July 2, 2018, response to IQVIA's First Set of Interrogatories. "Rule 26(g) does not require perfection and does not impose an unreasonably high burden on litigants. It simply requires that a reasonable inquiry be made into the factual basis of a discovery response and that responses to discovery be complete and correct when made." *Younes*, 312 F.R.D. at 706. While IQVIA believes that Veeva may have relied on the JIRA tickets when it provided its July 2, 2018, response to IQVIA's First Set of Interrogatories, the Special Master will not, without more evidence, infer that Veeva was aware of these JIRA tickets when it certified its responses. The JIRA tickets were generated very shortly before Veeva provided its responses and it is reasonable that Veeva may not have been acutely aware of the tickets when its responses were served. The Special Master is cognizant that this is a complex and contentious action in which millions of pages of document discovery have been exchanged.

However, the Special Master is more troubled by Veeva's failure to produce these JIRA tickets in response to Interrogatory No. 36 and IQVIA's motion to compel a response to

Interrogatory No. 36. While there is no dispute that Veeva accurately represented that its Hightail, FTP, Egnyte, Google e-mail/Google Drive, and NAS did not have logs or other electronic trails that would provide the exact date the data was deleted, a reasonable inquiry should have revealed the JIRA tickets.[14] Veeva has failed to provide any explanation for its delayed production of the JIRA tickets. These tickets were generated in June 2018 and yet they were not produced until February 2020, on the eve of the close of discovery after significant deposition discovery had been completed. Veeva appears to rely on its interpretation of Interrogatory No. 36, that Interrogatory No. 36 only sought audit trails documenting the exact date of deletion, however, as the Special Master has already indicated, Interrogatory No. 36 is not so limiting. The JIRA tickets provide information directly responsive to Interrogatory No. 36 and should have been produced.[15]

Veeva's lack of explanation for its failure to disclose the JIRA tickets in response to Interrogatory No. 36 and IQVIA's motion to compel make it exceedingly difficult for the Special Master to determine that a reasonable inquiry was made and thus, that the certification accompanying Veeva's response to Interrogatory No. 36 and Opposition to IQVIA's motion was objectively reasonable. Whether the failure to produce or disclose the JIRA tickets in response to Interrogatory No. 36 or in response to IQVIA's motion was the result of innocent oversight or something else, the Special Master must find that Veeva violated Rule 26(g). Furthermore, the Special Master finds that Veeva was required under Rule 26(e) to supplement its response to

[14] The Special Master sees nothing erroneous in the certifications of Patrick Young, Holly Stites, and Jonathan Johnston. The Special Master agrees with Veeva that those certifications spoke directly to the electronic systems those individuals were familiar with and there is no suggestion that their representations that these specific electronic systems did not have audit trail information that would provide the exact time a data extract was deleted were false.

[15] Even in light of Veeva's appeal of the Special Master's November 30, 2018, Order and its position that it need not produce its JIRA database until the appeal is decided, Veeva should have provided the information contained on the JIRA tickets in its custodians' possession in response to Interrogatory No. 36.

Interrogatory No. 36 once it became aware of the JIRA tickets, which were generated in June 2018. Again, Veeva has provided no explanation for its failure to produce or disclose the JIRA tickets in response to Interrogatory No. 36 aside from its unavailing assertion that Interrogatory No. 36 only sought audit trails demonstrating the exact time of deletion.

Rule 26(g) sanctions are mandatory unless the offending party's conduct was substantially justified. Substantial justification exists where reasonable people could differ. The test of substantial justification is satisfied if there is a genuine dispute concerning compliance. The Court can impose sanctions without finding that Veeva acted with subjective bad faith or purposely. This makes perfect sense because otherwise IQVIA would have to pay the price for Veeva's oversights.

Rule 37(c) then provides that if a party fails to provide information as required by Rule 26(e), that party is not allowed to use that information at trial, unless the failure was substantially justified or is harmless. Fed. R. Civ. P. 37(c)(1). In addition to or instead of this sanction, the court: (A) may order payment of the reasonable expenses, including attorney's fees, caused by the failure; (B) may inform the jury of the party's failure; and (C) may impose other appropriate sanctions, including any of the orders listed in Rule 37(b)(2)(A)(i)-(vi). Fed. R. Civ. P. 37(c)(1). Rule 37 is written in mandatory terms and is designed to provide a strong inducement for disclosure. *See Horizon Blue Cross Blue Shield of New Jersey*, 2015 WL 1137777 at *3.

The Special Master must now evaluate which sanctions are required based on Veeva's violations of Rule 26(g) and 37(e). The Special Master believes the appropriate remedy is to order Veeva to provide a response to Interrogatory No. 36, which includes JIRA ticket information in its possession for the forty deleted data extracts at issue.[16] In other words, Veeva

[16] There are forty-eight deleted data extracts at issue, however, JIRA tickets have already been produced for eight of the deleted data extracts.

is ordered to provide a response to Interrogatory No. 36, which includes JIRA ticket information for the forty deleted data extracts that have not been previously disclosed. If Veeva has the actual JIRA tickets in its possession it is ordered to produce those tickets to IQVIA. The Special Master is aware that Veeva has previously been ordered to produce certain Computer Forensic Discovery—including relevant portions of Veeva's JIRA trouble ticketing database. Veeva has appealed the Special Master's November 30, 2018, Order, and has to date refused to produce the relevant portions of the JIRA database while the appeal is pending. Nevertheless, the Special Master will order the production of the JIRA tickets related to the forty deleted data extracts that have not been produced to date as the Special Master finds them directly relevant to Interrogatory No. 36.

The Special Master will also recommend that Veeva be prohibited from introducing at trial the eight JIRA tickets it did produce in February 2020. Again, Veeva has not provided any explanation for its belated production of these eight JIRA tickets. While these tickets were produced before the close of fact discovery, they were produced after IQVIA would have been able to question witnesses as to the information contained on the tickets. In light of the fact that these tickets were generated in June 2018 and therefore in Veeva's possession well before February 2020, there is no reason these JIRA tickets should not have been produced earlier, especially in light of the fact that they are directly responsive to Interrogatory No. 36. "The purpose of the court system is to resolve civil disputes in a civil way. Thus, 'gotcha games' are not acceptable." *Inferrera v. Wal-Mart Stores, Inc.*, No. CIV. 11-5675 RMB/JS, 2011 WL 6372340, at *2 (D.N.J. Dec. 20, 2011) (internal citation omitted). Even if the delayed production of these tickets was not intentional, the delay has still prejudiced IQVIA by preventing it from questioning witnesses about these tickets. Accordingly, the Special Master recommends that the

District Court prohibit Veeva from introducing these eight tickets into evidence at the time of trial.

The Special Master will deny IQVIA's request for additional discovery, including the production of documents related to Veeva's preparation of its discovery responses and opposition to IQVIA's motion to compel. The Special Master will also deny IQVIA's request to depose representatives and counsel for Veeva related to the preparation of Veeva's discovery responses and opposition to IQVIA's motion to compel. The Special Master believes these requests are not appropriate and that any prejudice to IQVIA is adequately cured by the relief already ordered. The Special Master will not address the recovery sought by IQVIA improperly raised for the first time in its Reply.

The Special Master has also considered IQVIA's request for an award of fees and costs in its Sanctions Motion and Fraud Motion. In order to cure the unfairness to IQVIA, punish Veeva and deter such future conduct, the Special Master will grant IQVIA's request with respect to the Fraud Motion and the Sanctions Motion as it relates to the Genentech Incident, EUStage and James Kahan's e-mails. *See Folino*, 2018 WL 5982448 at *5. Within 60 days of the date of this Order, IQVIA is to supply a full accounting of relevant fees and costs so the Special Master can determine an appropriate award.

Conclusion

For the foregoing reasons, it is the opinion of the Special Master that IQVIA's Sanctions Motion, Privilege Motion, and Fraud Motion are GRANTED in part.

/s/ Dennis Cavanaugh
DENNIS M. CAVANAUGH, U.S.D.J. (Ret.)
Special Master

Date: May 7, 2021