ATTACHMENT A: Forensic Examination Protocol

This protocol relates to BioConvergence, LLC v. Jaspreet Attariwala, No. 1:20-mc-101-RC (D.D.C) ("D.C. Court"), which is a miscellaneous action relate to BioConvergence, LLC v. Jaspreet Attariwala, No. 1:19-cv-01745-SEB-MG (S.D. Ind.) (hereinafter, the "Underlying Action").

In accordance with the D.C. Court's instructions during the November 19, 2021 hearing, BioConvergence LLC d/b/a Singota Solutions ("Singota") has selected for initial inspection the external hard drive to which Simranjit J. Singh states he copied the Western Digital My Book drive that was identified by Rebecca Green and that Jaspreet Attariwala and Mr. Singh have testified was discarded in or about late 2017 or 2018 ("Western Digital My Book Drive"). See Declaration of Third Party, Sim J. Singh ("Singh Decl.") [Doc. 22-1] ¶¶ 34-35; Tr. Dep. Simranjit Attariwala, Nov. 4, 2021 ("Singh Dep.") at 116:4 – 119:15. Mr. Singh has stated that before discarding the Western Digital My Book Drive, he copied it to another external drive that remains in his possession (the "Device"). Singota therefore has selected that Device for initial inspection.

The examination shall be conducted by Jim Vaughn and iDiscovery Solutions (the "Examiner").

The Examiner will serve as an officer of the court in examining the Device and be bound by the terms of this Protocol. The Examiner will sign a copy of this Protocol and any Protective Order issued and in effect for this case at the time of the examination. The Examiner must agree in writing to be bound by the terms this Protocol or any order related to this examination prior to the commencement of the work.

The Examiner will abide by forensic industry ethical standards and will not accept improper attorney influence. Furthermore, the Examiner will not knowingly reach conclusions before research is completed, overstate conclusions, base conclusions and testimony on speculation, or give misleading testimony.

Singota has absolutely no interest in Mr. Singh's personal, family, or work data, and its only interest pertains to Singota's trade secrets or confidential information that belongs to Singota in completing their CDMO business (the "Relevant Singota ESI").

None of the sections in this Forensic Examination Protocol shall be construed as a waiver of any defense or privilege by Mr. Singh.

The following steps and reporting shall apply to the documentation, imaging and analysis of the external drive described by Mr. Singh on page 118 of his deposition transcript.

Step 1. Payment

1.1. Any charges and fees for the Examiner's professional time shall be timely paid exclusively by Plaintiff Singota per this Court's Order, subject to further order of this Court or the U.S. District Court for the Southern District of Indiana in which the underlying litigation is pending.

Step 2. Production of Device

2.1 Within 7 business days after this protocol has been approved by Judge Rudolph Contreras via Court Order, Mr. Singh shall ship the device to the Examiner using FedEx pack and ship services. FedEx will pack and ship the device. Mr. Singh's counsel will provide a copy of the tracking information for the shipment to Singota's counsel by email on the day of shipment.

2.2 All costs of shipping via FedEx will be borne by Mr. Singh. Mr. Singh will provide along with the Device the address and the contact information to be used for the return of the Device.

Step 3. Documentation

3.1 Upon receipt by the Examiner, the external device shall be photographed by the Examiner from enough angles to capture all markings of the device, including, but not limited to, the top, bottom, any connection ports and any attached labels or stickers. The make, model and serial number of the external device shall be documented and included in the report described in Section 4.4 of this protocol.

Step 4. Forensic Imaging

4.1 All forensic imaging must occur promptly in order for the Examiner to be able to comply with the Device return dates detailed in Step 5 below.

4.2 A forensic industry standard hardware write blocker shall be used to prevent any changes to the external device. Once connected to an industry standard hardware write blocker, a forensic imaging tool such as FTK Imager (or comparable software program) shall be used to create a full physical bit by bit forensic image. The write blocker and forensic imaging tool used shall be documented and included in the report as part of this protocol. The forensic image shall be verified by either SHA-1 or MD5 hash. An exact copy shall be made of the forensic image. The original forensic image shall be kept in pristine condition, and the copy shall be used for the analysis as described within this protocol.

4.3 The Examiner shall ensure that all partitions on the forensic image are accounted for. Once all partitions have been accounted for and are visible within the forensic image, recovery of folders and files shall be conducted. Once all partitions have been recovered, and all folders and files recovered, results of the analysis shall be placed into a report (the "Forensic Imaging Report").

4.4 The Forensic Imaging Report shall:

i. Contain the format date of the external drive.

ii. Except for 4.4(i), 4.4(vi), 4.4(vii), and 4.4(viii), be restricted to the time period from January 1, 2018, through the present (the "Relevant Time Period").

iii. Be restricted to files and emails with Creation Date, Last Accessed Date, Date Added, Last Modified / Last Saved / Last Written Date, within the Relevant Time Period.

iv. Contain a listing of files within the Relevant Time Period, minus content, in spreadsheet format, one file per row, to include File Name, File Extension, File Signature, File Size, Creation Date, Last Accessed Date, Date Added, Last Modified / Last Saved / Last Written Date, MD5 hash, Full Path values, Password Protection Status (yes or no), and File Description (archive, file, deleted, overwritten, etc.).

v. Contain a listing of emails within the Relevant Time Period, minus content, in spreadsheet format, one parent email and attachment name per row, to include sent date and time, from, to, cc, bcc, subject line and attachment name.

vi. If possible, provide an opinion regarding whether the Device is, or is not a copy of the Western Digital My Book Drive. If it is not possible to provide an opinion one way or the other, report what factors prevent the Examiner from providing an opinion.

vii. Report any evidence that tends to show what devices this Device has been connected to and when.

viii. Report any deletions from, manipulations of data on, and irregularities concerning the integrity of the Device.

4.5 The Report under this section shall be provided in full to Mr. Singh's counsel.

4.6 Only the Report's findings as to 4.4(i), 4.4(vi), 4.4(vii), and 4.4(viii) shall be provided to Singota's counsel.

Step 5. Return of the Device

5.1 Within 7 calendar days from the original date of receipt of the Device, and absent any reason beyond the control of the Examiner, the Examiner will immediately ship the original Device back to Mr. Singh by overnight delivery using FedEx ship services.

5.2 All costs of the return of the device via FedEx will be borne by Singota.

5.3 The return of device shall be made to the address and contact information provided by Mr. Singh. (See Section 2.2.)

5.4 Once the Device is returned, it shall not be utilized by Mr. Singh or connected to any other device until the procedures under this Protocol are completed, including any necessary remediation.

Step 6. Creation of Examiner List/Access to the Data

6.1 The Examiner has previously been provided or generated the following lists: Names of Singota's Clients, Names of Singota's Potential Clients, Names of Vendors Used by Singota, Names of Employees at Singota, and Metadata from Files originating on Ms. Attariwala's Singota work laptop, which the Examiner may refine with further input from Singota's counsel based on experiences using these search terms in the Underlying Action. This information is

confidential to Singota, and the Examiner shall continue to maintain the confidentiality of this information. (Hereafter, the "Confidential Search Term List.")

6.2 After creation of the forensic image and analysis image of the Device, the Examiner will run keyword searches using the Confidential Search Term List and use other data analytic tools, including metadata and digital fingerprint analysis, and use manual review, as it determines appropriate and consistent with industry best practices to attempt to identify Potentially Relevant Singota ESI for the Relevant Time Period and create a listing of identified Potentially Relevant Singota ESI files and emails (the "Examiner List"). The Examiner will prepare the Examiner List after the Examiner has completed the Forensic Imaging Report.

6.3 Within 30 calendar days of returning the Device to Mr. Singh, the Examiner will create the Examiner List and provide Mr. Singh's counsel and Singota's counsel with a copy of the Examiner List.

6.4 Within 30 calendar days of receipt of the Examiner List, Mr. Singh's counsel will use the Examiner List to create a log and a list of files and emails on the Examiner List that Mr. Singh believes in good faith contain entirely personal or privileged information. For each file or email included on the Examiner List that Mr. Singh claims to be entirely personal or privileged, Mr. Singh will provide a brief explanation of its contents and why it may have been captured by the Singota keyword searches. Mr. Singh's counsel will provide this log and list to Singota's counsel.

6.5 Within one business day after Mr. Singh's counsel has provided the log and list described in Section 6.4 to Singota's counsel, Mr. Singh's counsel will direct the Examiner to produce to Singota's counsel those files and documents identified on the Examiner List to which Mr. Singh has not objected as either privileged or personal. As soon as practicable after receiving Mr. Singh's direction, the Examiner will provide copies of those specified files and documents to Singota's counsel. This timeline can be extended by the agreement of the parties or by Court order due to, for example, the length of the list of files and emails.

6.6 Within 7 business days after Singota has received Mr. Singh's log and list under Section 6.4 and the production of files and emails pursuant to Section 6.5, Singota's counsel shall provide written notice to Mr. Singh's counsel whether Singota has any objections to Mr. Singh's withholdings based on claims of personal or privileged contents. If the parties cannot reach agreement on these matters, the parties shall meet and confer, and cooperate in good faith to resolve these objections. If the parties cannot resolve a dispute, then any party may move for protection or for an order for the Court to review specified documents in camera. If Singota requests such an in camera review by the Court, it will also provide an explanation as to why it challenges Mr. Singh's objection for each file or email. This timeline can be extended by the agreement of the parties or by Court order due to, for example, the length of the list of files and emails.

6.7 Within 15 business days after any objections have been resolved by agreement or court order, Singota's counsel shall confirm in writing whether each produced file contains Singota Relevant ESI. If no objection is raised by Singota, Singota's counsel shall confirm in writing to Mr. Singh's counsel whether each produced file contains Singota Relevant ESI within 15 business

days after receipt of the productions. This timeline can be extended by the agreement of the parties or by Court order due to, for example, the number of files and emails.

6.8 To the extent the Examiner has direct or indirect access to information protected by the attorney-client privilege, spousal/marital privilege, or any other privilege, such access will not result in a waiver of any privilege. The parties will meet and confer to attempt to agree to a protective order to cover any confidential files or documents of Mr. Singh or Singota from the Device produced under this protocol. Pending entry of such a protective order, possession of files and documents from the Device produced under this protocol is limited to the Examiner, the attorneys of record in this case, the parties, and their experts. Any files and documents from the Device produced under this protocol may be filed in the underlying or related litigation subject to any protective orders in place therein; neither party may file any such purportedly confidential information in any underlying or related litigation, however, until the Court has resolved any request for a protective order over the information.

Step 7. Remediation

7.1 If Relevant Singota ESI is found on the device, the parties will meet and confer to attempt to agree on a procedure for remediating the Relevant Singota ESI from the Device and any other copies in Mr. Singh's possession, custody, or control. If the parties are unable to agree, then the parties shall submit remediation proposals to the Court for the Court to decide the issue of remediation.

Step 8. Handling of Device Images Upon Conclusion of Examiner's Work

8.1 Once the parties have agreed or the Court has determined that all Relevant Singota ESI has been extracted from the device data in possession of the Examiner, the Examiner will within 15 business days destroy all other data in his possession, to include the Forensic Imaging Report, and provide a certificate to the parties stating such action. If this does not occur, upon the closing of this Third Party Matter (Case No. 1:20-mc-00101-RC), the Examiner will within 15 business days destroy all other data in his possession, to include the Forensic Imaging Report, and provide a certificate to the parties stating such action.

8.2 If Singota is unable to identify any Relevant Singota ESI in the device data in possession of the Examiner, then the Examiner shall proceed to the destruction of all data as described in Section 8.1.