

Source: *Martinelli v. Johnson & Johnson*, 2016 U.S. Dist. LEXIS 53146 (E.D. Cal., April 13, 2016).

## STIPULATED ESI AND HARD COPY PROTOCOL AND ORDER

The Parties hereby agree to the following protocol for production of electronically stored information ("ESI") and paper ("hardcopy") documents. Subject to the agreed upon Protective Orders in this Action, this protocol governs all productions in this action.

This protocol has the objective to facilitate the just, speedy, and inexpensive completion of discovery of ESI and hardcopy documents and to promote, whenever possible, the early resolution of disputes, including any disputes pertaining to scope or costs regarding the discovery of ESI without Court intervention. Nothing in this protocol shall limit a party's right to seek or object to discovery as set out in applicable rules, to rely on any Protective Order entered in this action concerning protection of confidential or otherwise sensitive information, or to object to the authenticity or admissibility of any hardcopy document or ESI produced in accordance with this protocol. The mere production of ESI as part of a mass production shall not itself constitute a waiver for any purpose.

### A. GENERAL AGREEMENTS

#### 1. Ongoing Cooperation among the Parties

The parties are aware of the importance the Court places on cooperation and commit to continue to consult and cooperate reasonably as discovery proceeds. The parties recognize that the failure of counsel or the parties to this action to cooperate in facilitating and reasonably limiting discovery requests and responses raises litigation costs and contributes to the risk of sanctions. The parties agree that their counsel's zealous representation of them is not compromised by conducting discovery in a cooperative manner.

#### 2. Proportionality

a. Reasonable Discovery Limits. The proportionality standard set forth in Rule 26(b)(2)(C) of the Federal Rules of Civil Procedure ("FRCP")<sup>1</sup> shall apply to discovery in this action. Consistent with that proportionality standard, the parties agree to cooperate in identifying and agreeing to appropriate limits on discovery, including limits on the number of custodians, discoverable data sources, and relevant time periods. The parties shall not be obligated to collect or produce ESI created after the date of filing of the initial complaint in this action.

b. Discoverable Custodians and Non-Custodial Data Sources. Consistent with the proportionality standard, within twenty-one (21) days after the Court's entry of this protocol, each party shall provide to the other party a list of the party's \_\_\_\_\_ (Example, twelve (12)) most likely custodians, as well as a list of non-custodial data

<sup>1</sup> Unless otherwise indicated, all statutory references herein are to the FRCP.

## Phase 7 – Review, Analyze, and Produce ESI and Paper

repositories whose reasonably accessible emails and other ESI the party will search for relevant information. Custodians shall be identified by name, title, dates of employment by the party, and a brief description of their employment duties. The parties agree to meet and confer in good faith in order to reach agreement on the lists of custodians whose emails and other ESI will be searched, and to agree upon such list (the "Final Custodian List") within fourteen (14) days of the date each party receives the other party's proposed list of \_\_\_\_\_ (Example, twelve (12)) most likely custodians. Absent a showing of good cause, and subject to any further agreement among the parties, the list(s) provided pursuant to this paragraph shall be the presumptive limit on permissible ESI discovery. If any custodian or data source identified on the Final Custodian List is located outside the United States, the parties shall meet and confer regarding such matters as relevancy and privacy of the data at issue and, as applicable, the timing of production of any such data.

c. Discovery Concerning Preservation and Collection Efforts. Discovery concerning the preservation and collection efforts of another party can contribute to unnecessary expense and delay and may inappropriately implicate work product and attorney-client privileged matters. If there is a dispute concerning the scope of a party's preservation or collection efforts, the parties or their counsel must meet and confer and fully explain their reason for believing additional efforts are, or are not, relevant and proportional pursuant to Rule 26(b)(1). In particular, before initiating discovery about preservation and collection, a party shall confer with the other party concerning the specific need for such discovery, including its relevance to claims and defenses, and the suitability of alternative means for obtaining the information.

d. On-Site Inspections of ESI. On-site inspections of ESI under Rule 34(b) shall be permitted only upon a good-faith showing by the requesting party of good cause and specific need or upon agreement of the parties. As appropriate, the Court may condition on-site inspections of ESI, as authorized in the preceding sentence, to be performed by independent third-party experts, and the Court may set other conditions it may deem appropriate.

e. Non-Discoverable ESI. Consistent with the proportionality standard set forth in the FRCP, absent a party's specific written notice for good cause, the following categories of ESI are presumed to be inaccessible and not discoverable:

- i. ESI deleted in the normal course of business before the time a preservation obligation in this action came into effect;
- ii. Backup data files that are maintained in the normal course of business for purposes of disaster recovery, including, but not limited to, backup tapes, disks, SAN, and other forms of media that are substantially duplicative of data that are more accessible elsewhere;
- iii. Deleted, "slack," fragmented, or unallocated data only accessible by forensics;
- iv. Random access memory (RAM), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system;
- v. On-line access data such as, (without limitation, temporary internet files, history files, cache files, and cookies;

**Attorney Work Product Prepared for Litigation**

**Phase 7 – Review, Analyze, and Produce ESI and Paper**

- vi. Data in metadata fields frequently updated automatically, such as last-opened or last-printed dates;
- vii. Electronic data (e.g., call logs, email, calendars, contact data, notes, and text messages) sent to or from mobile devices (e.g., iPhone, iPad, Android, and Blackberry devices), provided that copies of all such electronic data are routinely saved elsewhere (such as on a server, laptop, desktop computer, or 'cloud' storage);

**Attorney Work Product Prepared for Litigation**

- viii. Voicemail, including Telephone or VOIP voice messages;
- ix. Text messages and instant messages that are not retained in the ordinary course of business;
- x. SAS program and data files;
- xi. Server, system, network, or software application logs;
- xii. Data remaining from systems no longer in use that are unintelligible on the systems currently in use;
- xiii. Electronic data temporarily stored by laboratory equipment or attached electronic equipment, provided that such data are not ordinarily preserved as part of a laboratory report; and
- xiv. Structural files not material to individual file contents (e.g., .CCS, .XSL, .XML, .DTD, etc.).

f. Disaster-Recovery Backup Data. Consistent with the proportionality standard of the FRCP, absent a party's specific written notice for good cause, no party shall be required to modify or suspend procedures, including rotation of backup media, used in the normal course of business to back up data and systems for disaster recovery purposes. Absent a showing of good cause, such backup media shall be considered to be not reasonably accessible. Nothing in this provision obviates a party's duty to implement a litigation hold.

### 3. No Designation of Discovery Requests

Productions of hardcopy documents and ESI in the reasonably usable form set out in this protocol, including Attachment A, need not be organized and labeled to correspond to the categories in the requests.

### 4. Inadvertent Production

The inadvertent production of any emails, ESI, or other material constituting or containing attorney-client privileged information or attorney work-product, or which constitutes or contains information protected by any applicable privacy law or regulation, shall be governed by provisions contained in the Protective Order previously entered in this action.

## *B. ELECTRONICALLY STORED INFORMATION*

### 1. Production in Reasonably Usable Form

a. The parties shall produce ESI in reasonably usable form. Except as stated in paragraphs B.2 and B.3 below or as agreed hereafter by the parties, such reasonably usable form shall be the single-page TIFF-image format with extracted or OCR text and associated metadata as set out in Attachment A, which is incorporated in full into this protocol. If the receiving party for good cause explained in the request seeks production in native format of specifically identified ESI produced originally in TIFF-image form, the producing party shall respond reasonably and in good faith to any such request.

b. Redactions. The Producing Party may redact from any TIFF image, metadata field, or native file material that is protected from disclosure by applicable privilege or immunity, that is governed by Arizona \_\_\_\_ that the Protective Order entered in this Action allows to be redacted.

**Attorney Work Product Prepared for Litigation**

- c. Each party may make requests for good cause seeking production of specifically identified documents in color.

## 2. Electronic Spreadsheets, Presentations, Desktop, Databases, and Multimedia Files

Electronic spreadsheets (e.g., Excel), electronic presentations (e.g., PowerPoint), desktop databases (e.g., Access), and audio/video multimedia files that have been identified as responsive shall be produced in native format, unless they are authorized to be redacted in accordance with Paragraph 1.b above. After such redactions, the producing party either shall produce the redacted file in the reasonably usable form set out in Attachment A or shall produce the redacted copy in native format.

## 3. Enterprise Databases and Database Management Systems

In instances in which discoverable ESI in an enterprise database or database management system (e.g., Oracle, SQL server, DB2) can be produced in an already existing and reasonably available report, the parties shall collect and produce, in the reasonably usable TIFF-image form described in Attachment A, the discoverable material in that report format. If an existing report form is not reasonably available, the parties shall export from the original database discoverable information in a format compatible with Microsoft Excel or Microsoft Access, and the information shall be produced in that native format.

## 4. Additional Procedures for Native Format Files

- a. Procedures for assigning production numbers and confidentiality information to files produced in native format are addressed in Appendix A, incorporated herein, at Paragraph A.15.
- b. Any party seeking to use, in any proceeding in this action, files produced in native format shall do so subject to the following:
  - i. If the native file has been converted to TIFF-image or hardcopy, the original production number and confidentiality designation shall be stamped on each page of the resulting TIFF-image or hardcopy document representing the original native-format file, with a suffix added to the production number to identify the particular page in the file (e.g., XYZ00001\_001). In addition, the MD5 or SHA-1 hash value of the native file from which the TIFF-image or hardcopy document was generated shall be placed on the first page of the TIFF-image or hardcopy document;
  - ii. If the file will be used in its native format, the party seeking to use the native file shall first provide to other parties, sufficiently in advance of such use that the producing party can confirm that the file to be used is the same as the file produced, both the production number and the MD5 or SHA-1 hash value of the file; and
  - iii. Use of a file in native format, or use of a TIFF-image or hardcopy document representing the original native-format file shall constitute a representation that the file being used is an accurate and complete depiction of the original native-format file.

## 5. Use of Search Filters

a. To contain costs associated with the identification of relevant ESI for review and production, the parties may meet and confer to discuss either the use of reasonable search terms, file types, and date ranges, or the use of advanced search and retrieval technologies, including predictive coding or other technology-assisted review. The parties agree to meet and confer in good faith to reach agreement on a list of search terms and protocols for the production of ESI. During such discussions, the producing party shall retain the sole right and responsibility to manage and control searches of its data files. If the producing party makes revisions to

search terms or advanced technology procedures in order to make them more accurate and cost-effective, the producing party agrees to meet and confer with the requesting party regarding such revisions. A party's failure to meet and confer or to make a timely request for different or additional searches as described in this paragraph shall waive that party's right to object to the sufficiency of the searches actually conducted.

b. If, prior to the conduct of any searches, a receiving party believes in good faith that the producing party's decisions would result in deficiencies in production, the receiving party may make prompt, reasonable requests for different or additional searches. The producing party shall respond reasonably to such requests. Any proposed search terms shall be narrowly tailored to particular a issue. Indiscriminate terms, such as the producing party's name or its product names, are inappropriate unless combined with narrowing search criteria that sufficiently reduce the risk of over-inclusion.

c. The fact that any electronic file has been identified in agreed-upon searches shall not prevent any party from withholding such file from production on the ground that it is protected from disclosure by applicable privilege or immunity, that is protected from disclosure by Arizona \_\_\_\_\_ or that the Protective Order entered in this Action allows to be withheld.

d. Nothing in this section shall limit a party's right to seek reasonably agreement from the other parties or a Court ruling to modify previously agreed-upon search terms or procedures for advanced search and retrieval technologies.

e. The producing party shall propose an initial list of search terms to the requesting party. The parties agree to meet and confer in good faith to finalize a list of acceptable search terms within sixty (60) days of finalizing the Final Custodian List. Should the parties be unable to resolve any disputes cooperatively, they shall promptly bring their unresolved dispute(s) to the Court's attention.

f. The parties agree that a "hit" on a search term is not the sole factor in determining whether ESI is responsive to party's requests for production. For the avoidance of doubt, the producing party is not required to produce ESI containing a search term if the ESI is not otherwise responsive to a party's requests for production in this action, if it is protected from disclosure by applicable privilege, or that the Protective Order entered in this action allows the ESI to otherwise be withheld. The parties further agree that ESI that does not contain a "hit" on a search term may be excluded from production.

## 6. Email Threading

a. Email threads are email communications that contain prior or lesser-included email communications that also may exist separately in the party's electronic files. A most inclusive email thread is one that contains all of the prior or lesser-included emails, including attachments, for that branch of the email thread. The parties agree that removal of wholly-included, prior-in-time, or lesser-included versions from potential production will reduce all parties' costs of document review, production, and litigation-support hosting. Accordingly, each party may produce or list on any required privilege log only the most inclusive email threads.

b. Following production of the most inclusive email threads, and for good cause, a receiving party may make reasonable requests, with respect to most-inclusive email threads particularly identified in the requests, for metadata associated with individual prior or lesser-included emails within the identified most inclusive email threads. Upon such request, the producing party shall cooperate reasonably in responding to

any such requests.

7. Avoidance of Duplicate Production

"Duplicate ESI" means files that are exact duplicates based on the files' MD5 or SHA-1 hash values. The producing party need produce only a single copy of responsive Duplicate ESI. A producing party shall take reasonable steps to de-duplicate ESI globally (i.e., both within a particular custodian's files and across all custodians). Entire document families may constitute Duplicate ESI. De-duplication shall not break apart families. When the same Duplicate ESI exists in the files of multiple custodians, those persons shall be listed in the Custodian field identified in Paragraph A.14(c) of Attachment A.

*C. DOCUMENTS THAT EXIST ONLY IN HARDCOPY (PAPER) FORM*

A party may produce documents that exist in the normal course of business only in hardcopy form either (a) in their original hardcopy form, or (b) scanned and produced, with Bates numbers added and redacted as necessary in accordance with the procedures set out in Attachment A. Except as set out in section A.4 above, the scanning of original hardcopy documents does not otherwise require that the scanned images be treated as ESI.

DATED: \_\_\_\_\_, 20 \_\_

By: \_\_\_\_\_

Attorneys for \_\_\_\_\_

By: \_\_\_\_\_

Attorneys for \_\_\_\_\_

ORDER

The foregoing stipulation is hereby adopted by the Court and shall govern the production of electronically stored information and paper documents.

IT IS SO ORDERED. Dated: \_\_\_\_\_, 20 \_\_\_\_

\_\_\_\_\_ JUDGE UNITED STATES DISTRICT COURT

## ATTACHMENT A

*A1. Image Files.* Files produced in \*.tif format will be single page black and white \*.tif images at 300 DPI, Group IV compression. To the extent possible, original orientation will be maintained (i.e., portrait-to-portrait and landscape-to-landscape). Each \*.tif image will be assigned a unique name matching the production number of the corresponding page. Such files will be grouped in folders of no more than 1,000 \*.tif files each unless necessary to prevent a file from splitting across folders. Files will not be split across folders and separate folders will not be created for each file. Production ("Bates") numbers shall be endorsed on the lower right corner of all images. This number shall be a unique, consistently formatted identifier that will:

- a. be consistent across the production;
- b. contain no special characters; and
- c. be numerically sequential within a given file.

Bates numbers should be a combination of an alpha prefix along with an 8-digit number (e.g. ABC00000001). The number of digits in the numeric portion of the Bates number format should not change in subsequent productions. Confidentiality designations, if any, will be endorsed on the lower left corner of all images and shall not obscure any portion of the original file.

*A2. File Text.* Except where ESI contains text that has been redacted under assertion of privilege or other protection from disclosure, full extracted text will be provided in the format of a single \*.txt file for each file (i.e., not one \*.txt file per \*.tif image). Where ESI contains text that has been redacted under assertion of privilege or other protection from disclosure, the redacted \*.tif image will be OCR'd and file-level OCR text will be provided in lieu of extracted text. Searchable text will be produced as file-level multi-page UTF-8 text files with the text file named to match the beginning production number of the file. The full path of the text file must be provided in the \*.dat data load file. The text file shall include interlineated image keys/bates numbers sufficient to show for all TIFF-image pages, the bates-numbered page of the associated text.

*A3. Word Processing Files.* Word processing files, including without limitation Microsoft Word files (\*.doc and \*.docx), will be produced in the above format with tracked changes, comments, and hidden text showing.

*A4. Presentation Files.* To the extent that presentation files, including without limitation Microsoft PowerPoint files (\*.ppt and \*.pptx), are produced in \*.tif image format, such \*.tif images will display comments, hidden slides, speakers' notes, and similar data in such files.

*A5. Spreadsheet or Worksheet Files.* To the extent that spreadsheet files, including, without limitation, Microsoft Excel files (\*.xls or \*.xlsx), are produced in \*.tif image format, such \*.tif images will display hidden rows, columns, and worksheets, if any, in such files.

*A6. Parent-Child Relationships.* Parent-child relationships (e.g., the associations between emails and their attachments) will be preserved. Email and other ESI attachments will be produced as independent files immediately following the parent email or ESI record. Parent-child relationships will be identified in the data load file pursuant to paragraph A.14 below.

*A7. Dynamic Fields.* Files containing dynamic fields such as file names, dates, and times will be produced

**Attorney Work Product Prepared for Litigation**

showing the field code (e.g., "[FILENAME]" or "[AUTODATE]"), rather than the values for such fields existing at the time the file is processed.

*A8. English Language.* To the extent any data exists in more than one language, the data will be produced in English, if available. If no English version of a file is available, the producing party shall not have an obligation to produce an English translation of the data.

*A9. Embedded Objects.* Some Microsoft Office and .RTF files may contain embedded objects. Such objects typically are the following file types: Microsoft Excel, Word, PowerPoint, Project, Outlook, and Access; and PDF. Subject to claims of privilege and immunity, as applicable, objects with those identified file types shall be extracted as separate files and shall be produced as attachments to the file in which they were embedded.

*A10. Compressed Files.* Compressed file types (i.e., .CAB, .GZ, .TAR, .Z, .ZIP) shall be decompressed in a reiterative manner to ensure that a zip within a zip is decompressed into the lowest possible compression resulting in individual files.

*A11. Encrypted Files.* The producing party will take reasonable steps, prior to production, to unencrypt any discoverable electronically stored information that exists in encrypted format (e.g., because password-protected) and that can be reasonably unencrypted.

*A12. Scanned Hardcopy Documents*

a. In scanning hardcopy documents, multiple distinct documents should not be merged into a single record, and single documents should not be split into multiple records (i.e., hard copy documents should be logically unitized).

b. If a producing party is requested, and agrees, to provide OCR text for scanned images of hard copy documents, OCR should be performed on a document level and provided in document-level \*.txt files [\*21] named to match the production number of the first page of the document to which the OCR text corresponds. OCR text should not be delivered in the data load file or any other delimited text file.

c. In the case of an organized compilation of separate hardcopy documents—for example, a binder containing several separate documents behind numbered tabs—the document behind each tab should be scanned separately, but the relationship among the documents in the binder should be reflected in proper coding of the family fields set out below.

*A13. Production Numbering.*

In following the requirements of Paragraph A.1, the producing party shall take reasonable steps to ensure that attachments to documents or electronic files are assigned production numbers that directly follow the production numbers on the documents or files to which

<b>Field</b>	<b>Sample Data</b>	<b>Scanned Docs</b>
PRODBEG [Key Value]	ABC00000001	Yes
PRODEND	ABC00000008	Yes

**Attorney Work Product Prepared for Litigation**

they were attached. If a production number or set of production numbers is skipped, the skipped number or set of numbers will be noted. In addition, wherever possible, each \*.tif image will have its assigned production number electronically "burned" onto the image.

*A14. Data and Image Load Files.*

- a. Load Files Required. Unless otherwise agreed, each production will include [\*22] a data load file in Concordance (\*.dat) format and an image load file in Opticon (\*.opt) format.
- b. Load File Formats.
  - i. Load file names should contain the volume name of the production media. Additional descriptive information may be provided after the volume name. For example, both ABC001.dat or ABC001\_metadata.dat would be acceptable.
  - ii. Unless other delimiters are specified, any fielded data provided in a load file should use Concordance default delimiters. Semicolon (;) should be used as multi-entry separator.
  - iii. Any delimited text file containing fielded data should contain in the first line a list of the fields provided in the order in which they are organized in the file.
- c. Fields to be Included in Data Load File. For all documents or electronic files produced, the following metadata fields for each document or electronic file, if available at the time of collection and processing and unless such metadata fields are protected from disclosure by attorney-client or work-product privilege, or Arizona will be provided in the data load file pursuant to subparagraph (a), above, except to the extent that a document or electronic file has been produced with redactions. The term "Scanned Docs" refers to documents that are in hard copy form at the time of collection and have been scanned into \*.tif images. The term "Email and E-Docs" refers to files that are in electronic form at the time of their collection.

<b>Field</b>	<b>Sample Data</b>	<b>Scanned Docs</b>
PRODBEGATT	ABC00000009	Yes
PRODENDATT	ABC00001005	Yes
PRODCOUNTATT	2	Yes
CUSTODIAN	Smith, John	Yes
OTHER_CUSTODIANS	Doe, Jane; Jones, James	Yes
NATIVEFILE	Natives\001\001\	N/A ABC
FILEDESC	00000001.xls Microsoft Office	N/A

**Attorney Work Product Prepared for Litigation**

2007 Document

FOLDER	\\My N/A Documents\Docu ment1.doc	N/A
--------	---	-----

FILENAME	Document1.doc	N/A
----------	---------------	-----

DOEXT	DOC	N/A
-------	-----	-----

PAGES	2	Yes
-------	---	-----

AUTHOR	John Smith	N/A
--------	------------	-----

DATECREATED	10/09/2005	N/A
-------------	------------	-----

DATELASTMOD	10/09/2005	N/A
-------------	------------	-----

NAMELASTMOD	John Smith	No
-------------	------------	----

SUBJECT	Changes to Access Database	N/A
---------	-------------------------------	-----

FROM	John Beech	N/A
------	------------	-----

TO	Janice Birch	N/A
----	--------------	-----

<b>Field</b>	<b>Sample Data</b>	<b>Scanned Docs</b>
--------------	--------------------	---------------------

CC	Frank Maple	N/A
----	-------------	-----

BCC	John Oakwood	N/A
-----	--------------	-----

DATESENT	10/10/2005	N/A
----------	------------	-----

TIMESENT	10:33 am	N/A
----------	----------	-----

DATERCVD	10/10/2005	N/A
----------	------------	-----

TIMERCVD	10:33 am	N/A
----------	----------	-----

HASHVALUE	e4d909c290d 0fb1ca068ff addf22cbd0	No
-----------	--	----

**Attorney Work Product Prepared for Litigation**

CONFIDENTIALITY	HIGHLY CONFIDENTIAL	Yes
TEXTPATH	Text\001\001\ ABC00000001.txt	Yes
PRODVOL	VOL001	Yes

<b>Field</b>	<b>Email and E-Docs</b>	<b>Comment</b>
PRODBEG [Key Value]	Yes	Beginning production number
PRODEND	Yes	Ending production number
PRODBEGATT	Yes	Beginning production number of parent in a family
PRODENDATT	Yes	Ending production number of last page of the last attachment in a family
PRODCOUNTATT	Yes	The number of attachments associated with a family
CUSTODIAN	Yes	Custodian(s) that possessed the document or electronic file - multiple custodians separated by semicolon
OTHER_CUSTODIANS	Yes	When global de-duplication is used, these are custodians whose file has been de-duplicated
NATIVEFILE	Yes	Path and file name for native file on production media
FILEDESC	Yes	Description of the type file for the produced record.
FOLDER	Yes	Original source folder for the record produced.

<b>Field</b>	<b>Email and E-Docs</b>	<b>Comment</b>
FILENAME	Yes	Name of original electronic file as collected.
DOCEXT	Yes	File extension for email or e-doc

**Attorney Work Product Prepared for Litigation**

## Phase 7 – Review, Analyze, and Produce ESI and Paper

PAGES	Yes	Number of pages in the produced document or electronic file (not applicable to native file productions).
AUTHOR	Yes	Author information as derived from the properties of the document.
DATECREATED	Yes	Date that non-email file was created as extracted from file system metadata
DATELASTMOD	Yes	Date that non-email file was modified as extracted from file system metadata
NAMELASTMO	Yes	Last author of non-email file as extracted from file system metadata
SUBJECT	Yes	"Subject" field extracted from email message or metadata properties of the document
FROM	Yes	"From" field extracted from email message
TO	Yes	"To" field extracted from email
CC	Yes	message "Cc" or "carbon copy" field extracted from email message
BCC	Yes	"Bcc" or "blind carbon copy" field extracted from email message
DATESENT	Yes	Sent date of email message
TIMESENT	Yes	(mm/dd/yyyy format) Sent time of email message,
DATERCVD	Yes	time zone set to GMT Received date of email
TIMERCVD	Yes	message (mm/dd/yyyyformat) Received time of email message, time zone set to GMT
HASHVALUE	Yes	MD5 or SHA-1 hash value
CONFIDENTIALI	Yes	Text of confidentiality

**Attorney Work Product Prepared for Litigation**

**Phase 7 – Review, Analyze, and Produce ESI and Paper**

TEXTPATH	Yes	designation, if any Path to *.txt file containing extracted or OCR text
PRODVOL	Yes	Name of the Production Volume

*A15. Files Produced in Native Format.* Any electronic file produced in native file format shall be given a file name consisting of a unique Bates number and, as applicable, a confidentiality designation; for example, "ABC00000002\_[Original File Name]\_Confidential." For each native file produced, the production will include a \*.tif image slipsheet indicating the production number of the native file and the confidentiality designation, and stating "File Provided Natively". To the extent that it is available, the original file text shall be provided in a file-level multi-page UTF-8 text file with a text path provided [\*26] in the \*.dat file; otherwise the text contained on the slipsheet shall be provided in the \*.txt file with the text path provided in the \*.dat file.

*A16. Production Media.* Unless otherwise agreed, documents and ESI will be produced on optical media (CD/DVD), external hard drive, secure FTP site, or similar electronic format. Such media should have an alphanumeric volume name; if a hard drive contains multiple volumes, each volume should be contained in an appropriately named folder at the root of the drive. Volumes should be numbered consecutively (ABC001, ABC002, etc.). Deliverable media should be labeled with the name of this action, the identity of the producing Party, and the following information: Volume name, production range(s), and date of delivery.

*A17. Encryption of Production Media.* To maximize the security of information in transit, any media on which documents or electronic files are produced may be encrypted by the producing party. In such cases, the producing party shall transmit the encryption key or password to the requesting party, under separate cover, contemporaneously with sending the encrypted media. The receiving parties in this matter are on notice that certain data produced may originate from custodians in the European Union and the receiving parties therefore agree to follow the strictest security standards in guarding access to said data.