## UNITED STATES DISTRICT COURT NORTHERN DISTRICT OF FLORIDA PENSACOLA DIVISION

IN RE: DEPO-PROVERA (DEPOT
MEDROXYPROGESTERONE
ACETATE) PRODUCTS LIABILITY
LITIGATION

Case No. 3:25-md-3140

This Document Relates to: All Cases Judge M. Casey Rodgers Magistrate Judge Hope T. Cannon

# PRETRIAL ORDER NO. 13 (Governing Production of Documents and Electronically Stored Information)

This Order governs the production of documents and electronically stored information ("ESI") and will apply to all discovery of ESI and hard copy documents in this case, unless the Parties agree in advance and in writing or if this Order is modified by the Court.

Except as specifically set forth herein, this Order does not: (a) alter or affect the applicability of the Federal Rules of Civil Procedure ("Federal Rules") or any Local Rules of the U.S. District Courts ("Local Rules"), as applicable; (b) address, limit, determine, or affect the relevance, discoverability, or admissibility as evidence of any document or ESI, regardless of whether the document or ESI is to be preserved, is preserved, or is produced; or (c) alter or affect the objections to discovery available under the Federal Rules. The purpose of this Order is to facilitate the exchange of ESI and hard copy documents in an efficient manner and in accordance with the Federal Rules. By

### Page 2 of 22

stipulating to this Order and agreeing to produce documents, generally, in a particular form or forms, no Party waives any objections to producing any particular document or category of documents on any grounds whatsoever.

### I. Format for Defendants' Productions

This section governs the production of documents and ESI by Defendants Pfizer, Inc., Pharmacia & Upjohn Co. LLC, Pharmacia LLC, Greenstone LLC, Viatris, Inc., and Prasco LLC (collectively "Defendants") and applies to all discovery of ESI and hard copy documents by Defendants in this case, unless the Parties agree in advance and in writing or if this Order is modified by the Court.

1. <u>File Types and Formats</u>. All spreadsheet files (e.g., Microsoft Excel, Corel Quattro, etc.) must be produced as native files with TIFF placeholder images. All presentation files (e.g., Microsoft PowerPoint), image files (e.g., .jpg, .gif), and PDF files must be produced as native files with TIFF placeholder images, unless redactions are required, in which case such files must be produced as TIFFs. All word processing files (e.g., Microsoft Word) created or modified after January 1, 2023, must be produced as native files with TIFF placeholder images; word processing files last modified prior to January 1, 2023, and word processing files created or modified after that date for which redactions are required, must be produced as TIFFs. All media files, such as audio and video files, must be produced as native files with TIFF placeholder images. Emails must be produced as TIFFs. The Parties will meet and confer on the production of other file types. With respect to any ESI produced in TIFF format, the Producing Party must honor

### Page 3 of 22

reasonable requests from the Receiving Party for production of the associated native file. Files containing privileged information will be produced as redacted TIFF images.

2. <u>Native Files</u>. Any document produced in native file format must be given a file name consisting of a unique Bates number and, as applicable, a confidentiality designation; for example, "ABC0000002\_Confidential." For each native file produced, the production will include a \*.tiff 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 document text must be provided in a document-level multi-page UTF-8 with BOM text file with a text path provided in the \*.dat file; otherwise the text contained on the slipsheet language must be provided in the \*.txt file with the text path provided in the \*.dat file. Where redaction makes production of native-format files infeasible, the Parties will confer to determine a reasonably usable form for the production.

3. <u>TIFF Images</u>. Any document produced as TIFF images must be named according to the Bates number of the corresponding TIFF image. Each \*.tiff file should be assigned a unique name matching the Bates number of the corresponding image. All TIFF images should be provided in single-page, Group IV TIFF with a resolution of 300 DPI. Bates numbers and confidentiality designations should be electronically branded on each produced \*.tiff image. These \*.tiff images should be provided in a separate folder and the number of TIFF files per folder should be limited to 1,000 files.

Page 4 of 22

4. <u>Digital Photos</u>. Where reasonably possible, all digital photographs will be produced as full color image files in their native file format at their original resolution.

5. <u>Databases, Structured, Aggregated or Application Data</u>. The Parties will meet and confer to address the production and production format of any responsive data contained in a database or other structured or aggregated data source or otherwise maintained by an application. The Parties will reasonably cooperate in the exchange of information concerning such databases to facilitate discussions on productions and production format. If the Parties cannot reach agreement, the matter will be decided by the Court or its designee.

6. <u>Hard Copy Documents</u>. Documents that exist in hardcopy will be scanned to \*.tiff image format as set forth in Subsection I(3) above. Defendants' hard copy documents that are not text-searchable must be made searchable by OCR prior to production where possible. In scanning paper documents, distinct documents should not be merged into a single record, and single documents should not be split into multiple records (i.e., paper documents should be logically unitized<sup>1</sup>). In the case of an organized compilation of separate 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 compilation should be

<sup>&</sup>lt;sup>1</sup> Logical Unitization is the process of human review of each individual page in an image collection using logical cues to determine pages that belong together as documents. Such cues can be consecutive page numbering, report titles, similar headers and footers, and other logical indicators.

### Page 5 of 22

reflected in the proper coding of the beginning and ending document and attachment fields. Defendants will make their best efforts to unitize the documents correctly.

Short Message Communications. Short message communications (e.g., text 7. messages, WhatsApp, Slack, iMessage, Teams, G-Chat, Bloomberg, etc.) will be The TIFF image(s) must reflect the short message produced in TIFF format. communication thread for the full twenty-four day containing the short message communication, as well as the day(s) in the short message communication thread prior to or subsequent to such day that contain related or contextual content, or as may be necessary to demonstrate the inception or conclusion of the responsive conversation (the "complete communication thread"). The TIFF image of the complete communication thread must reveal and reflect the associated date, time, sender, recipient, and other persons included in the message/chat, and in-line representations of emojis plus inline references to any attachment, linked file, or embedded file revealed in the TIFF image of the communication/thread. Attachments, resolved linked files, and embedded files associated with any short message communication must be produced in accordance with subsections I(10) and I(12) hereof. Except for messages that contain privileged content, which may be redacted on the TIFF image in accordance with this Order, the complete communication thread will be produced. The Producing Party must honor reasonable requests from the Receiving Party for production of native short message communication files.

8. <u>De-NISTing</u>. Electronic files will be De-NISTed, removing commercially available operating system and application file information contained on the current NIST file list.

9. De-duplication. Defendants must make reasonable efforts to de-duplicate ESI. ESI produced by Defendants must be globally de-duplicated across all collected custodial and non-custodial sources. Documents are considered exact duplicates if a document family or stand-alone file has a matching MD5 or SHA-1 hash value as compared against the same document type (i.e., family or stand-alone file). Hash values of emails will be calculated on the concatenated values of at least the following fields: From, To, CC, BCC, Subject, Date Sent, Time Sent, Attachment Names, Body, and the hash values of all attachments. The names of all custodians and non-custodial sources who were in possession of a document prior to de-duplication will be populated in the ALL CUSTODIANS metadata field. The original file paths of a document prior to deduplication will be populated in the ALL FILE PATHS<sup>2</sup> metadata field. To account for and properly reflect the de-duplication (and thus removal) of duplicate documents in the possession of custodians and non-custodial sources for production waves/volumes following the initial production of a particular document, a meta-data overlay file must

<sup>&</sup>lt;sup>2</sup> ALL FILE PATHS metadata field must include the original file/folder paths, including file name for non-emails, where reasonably available, of all the locations where copies of the item were located at the time of collection, separated by semi-colons, in the order corresponding to the order of names in ALL CUSTODIANS. For emails collected from container files (e.g., .pst's), these include the original file paths of the container files and the location of the emails within the folder structure of the mail container/.pst from which it was collected, where reasonably available.

be periodically provided (no less than every two weeks, triggered by known changes to already produced documents) updating the ALL CUSTODIANS and ALL FILE PATHS meta-data fields for the initially produced version of the duplicate document with any additional de-deduplicated CUSTODIANS and ALL FILE PATHS.

10. <u>Embedded Files</u>. Embedded files, except for images embedded in emails, are to be produced as family groups. Embedded files should be assigned Bates numbers that directly follow the Bates numbers on the documents within which they are embedded.

11. <u>Dynamic Fields</u>. Documents with dynamic fields for file names, dates, and times will be processed to show the field code (e.g., "[FILENAME]"), rather than the values for such fields existing at the time the file is processed.

12. <u>Parent-Child Relationships.</u> For document families, the parent-child relationships—the association between the parent document and the attached document and/or linked file—should be preserved. Attachments/linked files should be consecutively produced with the parent document that attached/referenced them.

13. <u>Time Zone</u>. All provided metadata pertaining to dates and times will be standardized to UTC.

14. <u>Bates Numbering</u>. Bates numbering should be consistent across the production, contain no special characters, and be numerically sequential within a given document. If a Bates number or set of Bates numbers is skipped, the skipped number or set of numbers should be noted with a placeholder. Attachments to documents will be

### Page 8 of 22

assigned Bates numbers that directly follow the Bates numbers on the documents to which they were attached. In addition, wherever possible, each \*.tiff image will have its assigned Bates number electronically "burned" onto the image. The Bates number must:

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

15. <u>Excluded File Types</u>. Absent a particularized need and good cause showing, the Parties agree that there is no need to collect ESI from the following sources:

- a. Deleted, slack, fragmented, or other data only accessible by forensics;
- b. Random access memory (RAM), temporary files, or other data difficult to preserve without disabling the operating system;
- c. On-line access data such as temporary internet files, history, cache, cookies, and the like;
- d. Back-up data that is duplicative of data that can be collected elsewhere; and
- e. Server, system, or network logs.

16. <u>Redactions</u>. No redactions for relevance may be made within a produced document or ESI item. Any redactions must be clearly indicated on the face of the document, with each redacted portion of the document stating that it has been redacted and the basis for the redaction, and a metadata field must indicate that the document contains redactions and the basis for the redaction (e.g., "A/C Privilege"). Where a responsive document contains both redacted and non-redacted content, Defendants must

### Page 9 of 22

produce the remainder of the non-redacted portions of the document and the text/OCR corresponding to the non-redacted portions.

- a. <u>Spreadsheets</u>. Spreadsheet files requiring redaction for information other than privilege, including Microsoft Excel files, will be redacted within the native file, and the redacted native file will be produced as provide herein.
- b. Other Documents. All native files that require redaction must first be processed to show and reveal all color, comments, revision marks, speaker notes, or other user-entered data which are visible in any view of the document in its native application, all of which must be evident in the generated TIFF image(s). Where reasonably possible, any occurrences of date/time auto-field items, including in headers and footers, will be removed and replaced with the term AUTODATE to prevent the current date from being printed. Email header information (e.g. date, subject line, etc.) should not be redacted unless it is independently privileged. The production of a document in a redacted form does not affect Defendants' obligation to timely assert and substantiate the assertion of privilege over the content in a privilege log. Defendants must honor reasonable requests for the production of particular redacted documents in other formats where the TIFF image is not reasonably usable. Redacted versions of documents that contained color in their un-redacted form must be produced in color in TIFF format.

17. <u>Load File Formats</u>. ESI will be produced with a standard Concordance (\*.dat) load file format and an image load file that is in .OPT format. The Concordance (\*.dat) load file must be provided with UTF-8 encoding.

18. <u>Metadata to Be Produced</u>. The metadata fields detailed in Exhibit A should be produced for each document to the extent that such information is available or, in the case of metadata created during processing such as Bates numbers, created, at the time of collection and processing, except that if a field contains privileged information, that privileged information may be redacted and noted in a corresponding privilege log.

19. <u>Extracted Text and OCR</u>. Each document, whether produced in Native or in TIFF format, and whether originally existing in electronic or in hard copy, must be produced with extracted text or OCR, as described herein.

a. <u>Extracted Text (Emails, Short Message Communications, Unredacted Native ESI, and Redacted Spreadsheets</u>). All email, short message communications, un-redacted native ESI, and redacted spreadsheets produced as native files, should be provided with complete document-level extracted text files. Extracted text must include all comments, revisions, tracked changes, speaker's notes, embedded URLs, and text from documents with comments or tracked changes, and hidden and very hidden worksheets, slides, columns and rows. Text extracted from emails must include all header information that would be visible if the email was viewed in Outlook including: (1) the individuals to whom the communication was

directed ("To"), (2) the author of the email communication ("From"), (3) who was copied and blind copied on such email ("CC" and "BCC"), (4) the subject line of the email ("RE" or "Subject"), (5) the date and time of the email, (6) the text of any embedded URLs, and (7) the names of any attachments.

b. OCR (Redacted Native ESI, Hard Copy Documents). In the event a document other than spreadsheets, e.g., Excel files, contains text that is to be redacted, Optical Character Recognition ("OCR") text files should be provided for any un-redacted portions of the documents. Document-level OCR text files must also be provided for all hard copy scanned documents. OCR software must be set to the highest quality setting for any previously unscanned paper documents, and reasonable quality control measures must be used to ensure that the integrity of scanned copies of previously unscanned paper documents are preserved for OCR (e.g., pages are not angled or skewed, text is not blurred or obscured, etc.). Documents containing foreign language text must be OCR'd using the appropriate settings for that language (e.g., OCR of German documents must use settings that properly capture umlauts and OCR of Asian language documents must properly capture the relevant Asian characters). Settings such as "auto-deskewing" and "auto-rotation" must be turned on during the OCR process to maximize text recognition on any given page.

c. <u>Format of Extracted Text and OCR</u>. The extracted full text and/or OCR text for all deliverables should be in separate document-level, UTF-8 with BOM encoded TXT files provided in a separate folder. The number of TXT files per folder should be limited to 1,000 files.

20. <u>Encryption</u>. To maximize the security of information in transit, any media or file sharing electronic document repository on which documents are produced must be encrypted by Defendants. Production deliverables provided via File Transfer Protocol ("FTP") must be made available on a secured FTP connection with AES 256-bit encryption. All production volumes uploaded by Defendants via this file sharing document repository must remain available for download for no less than thirty (30) calendar days. In such cases, the Defendants must transmit the encryption key or password to a requesting Party, under separate cover, contemporaneously with sending the encrypted media, or correspondence indicating the availability of the encrypted FTP deliverables.

### II. Protocol for Search/Identification of Responsive Documents

21. The Parties have been meeting-and-conferring, and agree to continue to meet and confer, concerning the potential use of TAR, other enhanced search techniques and protocols, and validation processes and protocols to facilitate Defendants' identification of responsive documents for production. The Parties must submit their joint proposed search and validation protocol, or points of dispute for resolution by the Court, by March 21, 2025.

Page 13 of 22

### **III.** Production Format for Plaintiffs' Productions

22. The Parties anticipate that the production and production format of Plaintiffs' case-specific materials will be the subject of a future Court order. Absent further agreement or order of the Court, Plaintiffs' counsel must produce case-specific materials in native file format, PDF, or such other reasonably useable format that retains the relevant characteristics of the original document. Any document that requires redaction must be produced in image format, e.g., TIFF or PDF. All of Plaintiffs' production documents must be uniquely named.

23. For document families, the parent-child relationships—the association between the parent document and the attached document and/or linked file—should be preserved. Attachments/linked files should be consecutively produced with the parent document that attached/referenced them.

24. To the extent Plaintiffs produce a document other than in native format, and Defendants request metadata or other information, the Parties must reasonably confer about an alternative production format for such document, including the necessity for such alternative production format. Any such request by a Defendant must be specific and targeted.

## IV. Provisions Applicable to Both Plaintiffs' and Defendants' Productions.

25. <u>Known Responsive Material Must Be Produced</u>. ESI and hardcopy documents that are known to Plaintiffs' Counsel or Defendants' Counsel to be non-privileged and responsive to a discovery request must be produced without regard to

Page 14 of 22

whether it was responsive to a search term, of high "relevance" by a TAR text classification algorithm, or otherwise flagged as potentially responsive by another search technique, unless Counsel specifically identifies the documents as being withheld pursuant to a specific objection.

26. <u>Discrete Document Collections</u>. Those portions of a Plaintiff's or Defendant's documents that represent discrete document collections, such as substantially relevant folders of ESI specifically segregated by Defendants, Defendants' employees, or Plaintiffs, before or after the commencement of this litigation, that are substantially relevant to the claims and defenses in this proceeding, must be reviewed for responsiveness (subject to appropriate claims of privilege) without regard to whether a given document in the collection is responsive to a search term, of high "relevance" by a TAR text classification algorithm, or otherwise flagged as potentially responsive by another search technique.

27. <u>Unsearchable Documents</u>. Documents that are reasonably believed to be responsive and for which text-based search technologies are fundamentally ineffective, such as images, spreadsheets, etc. must be reviewed without culling by search terms, predictive coding, or other technologies that rely primarily on text.

28. <u>Use of Other Technology or Methodology</u>. Prior to use or further use by any Party other than as specified within this protocol or the upcoming supplement regarding a protocol for the identification of and search for responsive documents, the Parties must meet and confer to disclose and discuss any proposed use of software or

### Page 15 of 22

other technologies used to identify or eliminate sources of potentially responsive documents, including keyword or Boolean searching, file type culling, de-duplication, filtering, near de-duplication, e-mail thread suppression, clustering or concept searching. Use of such technologies to reduce the volume of materials to be collected or reviewed, other than as described within this document, requires the opposing party's consent and will be subject to a separate mutually agreed-upon stipulation or Order of the Court setting forth the protocol for the use of such technologies as negotiated by the Parties.

29. <u>Additional or Alternate Methodologies for Documents from Certain</u> <u>Custodians and Non-Custodial Data Sources</u>. The Parties will meet and confer to address the need for and implementation of additional or alternate methodologies for identifying possibly responsive documents from custodians and non-custodial data sources that may warrant such treatment.

30. <u>Mobile and Handheld Device Documents and Data</u>. If responsive data that can reasonably be extracted and produced in the formats described herein is identified on a mobile or handheld device, that data must be produced in accordance with the generic provisions of this protocol. To the extent that responsive data identified on a mobile or handheld device is not susceptible to normal production protocols, the Parties will meet and confer to address the identification, production, and production format of any responsive documents and data contained on any mobile or handheld device.

31. <u>ESI Liaisons</u>. To promote transparency, communications, and cooperation among the Parties, the Parties must designate e-discovery liaisons for purposes of

### Page 16 of 22

meeting and conferring on ESI topics. As proposed by the Parties, the ESI liaison for Plaintiffs will be David Buchanan and the ESI liaison for Defendants will be Jessica Rydstrom, or their designees. All productions of ESI by any Party or non-party must be sent to the Parties' respective ESI liaison and lead counsel, and any identified designees.

32. <u>Impact of Order on Other Obligations</u>. Nothing in this agreement affects the preservation requirements set forth in previous orders, subsequent orders, or any other preservation obligations of the Parties for these proceedings or for other purposes, such as pursuant to court order, administrative order, statute, or in response to other anticipated litigation. By preserving documents or ESI for the purpose of this litigation, the Parties are not conceding that such material is discoverable, nor are they waiving any claim of privilege.

33. <u>Continuing Obligations</u>. The Parties will continue to meet and confer regarding any issues as necessary and appropriate, including agreeing to modify any of the dates and periods set forth in this Order. This Protocol does not address or resolve any objections to the scope of the Parties' respective discovery requests.

34. <u>Reservation of Rights</u>. The Parties retain the right, upon reviewing any productions made by another Party in this Action or conducting other investigation and discovery, to request that Documents from additional non-custodial data sources and custodians be produced. The Parties must meet and confer regarding such request(s) prior to any search or production related thereto.

### Page 17 of 22

35. <u>Document Storage</u>. During the pendency of this litigation, the Parties must make reasonable efforts to preserve the originals of all hard copy and ESI documents produced to the opposing Parties and to preserve the original native format version of any ESI produced in non-native format.

36. <u>Good Faith Compliance and Conferral Obligation</u>. The Parties must make good faith efforts to comply with and resolve any differences concerning compliance with this Order. No Party may seek relief from the Court concerning compliance with this Order unless it has first conferred with the other Parties. The Parties are required to reasonably cooperate in the exchange of information concerning data systems and ESI as may be necessary to facilitate the discovery and exchange of ESI in these proceedings and to further the exchange of information commenced at the Parties' Rule 26(f) Conference.

37. <u>Non-English Documents</u>. To the extent that Documents are produced that contain languages other than English, in whole or in part, the Producing Party must produce each such Document in the original language or languages in which it was written when collected. The Producing Party has no obligation to create a translation of the Documents, or any portion thereof, but must provide any translation of the Document or any portion thereof that exists or is created through machine translation prior to production of the Document.

38. <u>Alternate Formats</u>. Notwithstanding the Parties' stipulations herein, upon reasonable request made by the Receiving Party, the Parties must confer regarding the

Page 18 of 22

production in an alternate format of a document previously produced in accordance with this order.

39. <u>Effect of Order</u>. The Parties' agreement to this Order is without prejudice to the right of any Party to seek an order from the Court to rescind or amend this Order for good cause shown. Nothing in this Order abridges the rights of any person to seek judicial review or to pursue other appropriate judicial action with respect to any discovery ruling made by the Court in this matter.

SO ORDERED this 14th day of March, 2025.

<u>M. Casey Rodgers</u>

M. CASEY RODGERS UNITED STATES DISTRICT JUDGE

Page 19 of 22

## ATTACHMENT A<sup>3</sup>

Field	Definition
CUSTODIAN	Name of person or other data source (non-human) from where documents/files are produced. Where redundant names occur, individuals should be distinguished by an initial which is kept constant throughout productions (e.g., Smith, John A. and Smith, John B.).
ALLCUSTODIANS	Identification of any additional custodians for duplicate files or email messages
BEGBATES	Beginning Bates Number (production number)
ENDBATES	Ending Bates Number (production number)
PGCOUNT	Number of pages in the document
FILESIZE	File Size
APPLICATION	Commonly associated application for the specified file type.
FILEPATH	Original file/path of the location where the item was located at the time of collection. This should include location, and, for e-documents and e-attachments, file name, and file extension. Folder names and path should be included, and, for emails and attachments collected from a container such as a .pst, the full folder path within the container. Any container names should be included in the path.

 $<sup>^3</sup>$  The fields listed in this Attachment A should be included for documents produced where the metadata is available and reasonably collectable or where it can be reasonably added. The Parties recognize that not every document produced will be produced with all available data – e.g., one off collections from targeted sources may not be reasonable to collect forensically in order to preserve all available metadata. To the extent a document is produced missing certain metadata, and the metadata is necessary to understand the context of the document, a Receiving Party may request a Producing Party conduct a reasonable investigation as to why the metadata is missing. No reasonable request for such investigation will be denied.

ALLFILEPATHS	Original file/path of the location where duplicate items were located at the times of collection. This should include location, and, for e-documents and e-attachments, file name, and file extension. Folder names and path should be included, and, for emails and attachments collected from a container such as a .pst, the full folder path within the container. Any container names should be included in the path.
FILENAME	Original file name at the point of collection
NATIVEFILELINK	For documents provided in native format only
TEXTPATH	File path for OCR or Extracted Text files
MSGID	Email system identifier assigned by the host email system. This value is extracted from parent message during processing
FROM	Sender
ТО	Recipient
CC	Additional Recipients
BCC	Blind Additional Recipients
SUBJECT	Subject line of e-mail
PARENTMSGID	Where the item is an email which is a REPLY or FORWARD, the MSGID of the original email which was REPLIED to or FORWARDED
CONVERSATIONID	Email thread identifier
ATTACHBATES	Bates number from the first page of each attachment
BEGATTACH	First Bates number of family range (i.e., Bates number of the first page of the parent e-mail or document)
ENDATTACH	Last Bates number of family range (i.e., Bates number of the last page of the last attachment or, if no attachments, the document itself)
ATTACHCOUNT	Number of attachments to an e-mail

ATTACHNAMES	Names of each individual Attachment, separated by semi-colons delimited by unique character
PRODVOL	Name of media that data was produced on.
DATESENT (mm/dd/yyyy hh:mm:ss AM)	Date Sent
DATERCVD (mm/dd/yyyy hh:mm:ss AM)	Date Received
E-MAILDATSORT (mm/dd/yyyy)	Sent Date of the parent e-mail (most recent e-mail in a chain)
E-MAILOUTLOOKTYPE	Type of Outlook item, e.g., e-mail, calendar item, contact, note, task (Outlook or similar system data)
HASHVALUE	MD5 hash value
TITLE	Internal document property
AUTHOR	Internal document property
DATECRTD (mm/dd/yyyy hh:mm:ss AM)	Creation Date
LAST MODIFIED BY	Last person who modified (saved) a document
LASTMODD (mm/dd/yyyy hh:mm:ss AM)	Last Modified Date
REDACTED	"Redacted" must be indicated with a Y/N.
REDACTIONREASON	Basis of redaction. If more than one, separate reasons by semi- colons
HASREVISIONS <sup>4</sup>	Y if a Word document with revisions, otherwise N or empty
HASCOMMENTS	Y if a Word or Excel document with comments, otherwise N or empty
HASHIDDENTEXT	Y if a Word document with hidden text, otherwise N or empty

<sup>&</sup>lt;sup>4</sup> Defendants advise that their ESI processing platform does not provide the requested meta-data for certain requested fields (noted in bold and italic in this attachment): i.e., HASREVISIONS, HASCOMMENTS, HASHIDDENTEXT, HASVERYHIDDENWORKSHEETS. The Parties are required to confer, and in the event Defendants' processing platform cannot generate such information, those fields may be excluded from the meta-data deliverable.

Page 22 of 22

HASHIDDENSLIDES	Y if a PowerPoint document with hidden slides, otherwise N or empty
HASSPEAKERNOTES	Y if a PowerPoint document with speaker's notes, otherwise N or empty
HASHIDDENROWS	Y if an Excel document with hidden rows, otherwise N or empty
HASHIDDENCOLUMNS	Y if an Excel document with hidden columns, otherwise N or empty
HASHIDDENWORKSHEETS	Y if an Excel document with hidden worksheets, otherwise N or empty
HASVERYHIDDENWORKS	Y if an Excel document with very hidden worksheets, otherwise
HEETS	N or empty
DOCUMENTTYPE	Descriptor for the type of document: <b>"E-document"</b> for electronic documents not attached to e-mails; <b>"E-mail"</b> for all e-mails; <b>"E-attachment"</b> for files that were attachments to e- mails; and <b>"Physical"</b> for hard copy physical documents that have been scanned and converted to an electronic image.
IMPORTANCE	High Importance – indicates Priority E-mail message.
CONFIDENTIALITY TREATMENT	Confidentiality treatment level
TRANSLATION	Translation of any foreign language text (Y/N)