Doc. 61

B. ESI Disclosures

Within 45 days of entry of this Order, or at a later time if agreed to by the parties, each party shall disclose:

- 1. <u>Custodians.</u> The custodians most likely to have discoverable ESI in their possession, custody, or control. The custodians shall be identified by name, title, connection to the instant litigation, and the type of the information under the custodian's control.
- 2. <u>Non-custodial Data Sources.</u> A list of non-custodial data sources (*e.g.*, shared drives, servers), if any, likely to contain discoverable ESI.
- 3. <u>Third-Party Data Sources.</u> A list of third-party data sources, if any, likely to contain discoverable ESI (*e.g.*, third-party email providers, mobile device providers, cloud storage) and, for each such source, the extent to which a party is (or is not) able to preserve information stored in the third-party data source.
- 4. <u>Inaccessible Data.</u> A list of data sources, if any, likely to contain discoverable ESI (by type, date, custodian, electronic system or other criteria sufficient to specifically identify the data source) that a party asserts is not reasonably accessible under Fed. R. Civ. P. 26(b)(2)(B).
- 5. <u>Foreign data privacy laws.</u> Nothing in this Order is intended to prevent either party from complying with the requirements of a foreign country's data privacy laws, *e.g.*, the European Union's General Data Protection Regulation (GDPR) (EU) 2016/679. The parties agree to meet and confer before including custodians or data sources subject to such laws in response to any ESI or other discovery request.

C. ESI Discovery Procedures

ORDER REGARDING DISCOVERY OF

ELECTRONICALLY STORED INFORMATION

PAGE - 2

(Case No. 2:22-CV-00910-RSM)

ORDER REGARDING DISCOVERY OF ELECTRONICALLY STORED INFORMATION

iii.

PAGE - 3

(Case No. 2:22-CV-00910-RSM)

1. <u>On-site inspection of electronic media.</u> Such an inspection shall not be required absent a demonstration by the requesting party of specific need and good cause or by agreement of the parties.

- 2. <u>Search methodology.</u> The parties shall timely confer to attempt to reach agreement on appropriate search terms and queries, file type and date restrictions, data sources (including custodians), and other appropriate computer- or technology-aided methodologies, before any such effort is undertaken. The parties shall continue to cooperate in revising the appropriateness of the search methodology.
 - a. Prior to running searches:
- i. The producing party shall disclose the data sources (including custodians), search terms and queries, any file type and date restrictions, and any other methodology that it proposes to use to locate ESI likely to contain responsive and discoverable information. The producing party may provide unique hit counts for each search query, including hit counts by custodian, providing that it can be done with minimal burden.
- ii. After disclosure, the parties will engage in a meet and confer process regarding additional terms sought by the non-producing party.

requesting party. Focused terms and queries should be employed; broad terms or queries, such

as product and company names, generally should be avoided. A conjunctive combination of

The following provisions apply to search terms / queries of the

term unless they are variants of the same word. The producing party may identify each search term or query returning overbroad results demonstrating the overbroad results and a counter proposal correcting the overbroad search or query.

b. Upon reasonable request, a party shall disclose information relating to network design, the types of databases, database dictionaries, the access control list and security access logs and rights of individuals to access the system and specific files and applications, the ESI document retention policy, organizational chart for information systems personnel, or the backup and systems recovery routines, including, but not limited to, tape rotation and destruction/overwrite policy.

3. Format.

- a. ESI will be produced to the requesting party with searchable text, in a format to be decided between the parties. Acceptable formats include, but are not limited to, native files, multi-page TIFFs (with a companion OCR or extracted text file), single page TIFFs (only with load files for e-discovery software that includes metadata fields identifying natural document breaks and also includes companion OCR and/or extracted text files), and searchable PDF.
- b. Unless otherwise agreed to by the parties, files that are not easily converted to image format, such as spreadsheet, database, audio, video, and drawing files, will be produced in native format.
- c. Each document image file shall be named with a unique number (Bates Number). Documents produced in native format will be assigned a Bates Number and be produced with a corresponding load file. File names should not be more than twenty characters long or contain spaces. When a text-searchable image file is produced, the producing party must

ORDER REGARDING DISCOVERY OF ELECTRONICALLY STORED INFORMATION

PAGE - 4

(Case No. 2:22-CV-00910-RSM)

3

5

6 7

8

10

11

12

13 14

15

16

17

18

20

19

21

22

23

24

25

below) and, where applicable, the revision history.

- d. If a document is more than one page, the unitization of the document and any attachments and/or affixed notes shall be maintained as they existed in the original document.
- The full text of each electronic document shall be extracted ("Extracted Text") and produced in a text file. The Extracted Text shall be provided in searchable ASCII text format (or Unicode text format if the text is in a foreign language) and shall be named with a unique Bates Number (e.g., the unique Bates Number of the first page of the corresponding production version of the document followed by its file extension). For any redacted documents that are produced as images, the Producing Party will also provide OCR text files for the nonredacted portions of those documents.
- 4. <u>De-duplication</u>. The parties may de-duplicate their ESI production across custodial and non-custodial data sources after disclosure to the requesting party, and the duplicate custodian information removed during the de-duplication process shall be tracked in a duplicate/other custodian field in the database load file. If processing and production is done on a rolling basis, an updated Duplicate Custodians field with additional values shall be provided in an overlay. The producing party shall identify whether the overlay replaces previously produced fields for a file or supplements them.
- 5. Email Threading. The parties may use analytics technology to identify email threads and need only produce the unique most inclusive copy and related family members and may exclude lesser inclusive copies. However, in all events the producing party shall produce all copies of emails or email threads with attachments, whether they are the unique most inclusive copy and related family members, or whether they are lesser inclusive copies. Upon reasonable request, the producing party will produce a less inclusive copy or, upon reasonable request,

ORDER REGARDING DISCOVERY OF ELECTRONICALLY STORED INFORMATION

PAGE - 6

(Case No. 2:22-CV-00910-RSM)

missing metadata, if, for example, a threaded email cuts off to/from/cc/subject line/date information, or, upon reasonable request, both.

- 6. Metadata fields. If the requesting party seeks metadata, the parties agree that only the following metadata fields need be produced, and only to the extent it is reasonably accessible and non-privileged: document type; custodian and duplicate custodians (or storage location if no custodian); author/from; recipient/to; cc and bcc; title/subject; email subject; file name; file size; file extension; original file path; date and time created, sent, modified and/or received; and hash value. The list of metadata type is intended to be flexible and may be changed by agreement of the parties, particularly n light of advances and changes in technology, vendor, and business practices.
- 7. Hard-Copy Documents. If the parties elect to produce hard-copy documents in an electronic format, the production of hard-copy documents will include a cross-reference file that indicates document breaks and sets forth the custodian or custodian/location associated with each produced document. Hard-copy documents will be scanned using Optical Character Recognition technology and searchable ASCII text files will be produced (or Unicode text format if the text is in a foreign language), unless the producing party can show that the cost would outweigh the usefulness of scanning (for example, when the condition of the paper is not conducive to scanning and will not result in accurate or reasonably useable/searchable ESI). Each file will be named with unique Bates Number (e.g. the unique Bates Number of the first page of the corresponding production version of the document followed by its file extension).

D. Preservation of ESI

The parties acknowledge that they have a common law obligation, as expressed in Fed. R. Civ. P. 37(e), to take reasonable and proportional steps to preserve discoverable information in the party's possession, custody, or control. With respect to preservation of ESI, the parties agree as follows:

- 1. Absent a showing of good cause by the requesting party, the parties shall not be required to modify the procedures used by them in the ordinary course of business to back-up and archive data; provided, however, that the parties shall preserve all discoverable ESI in their possession, custody, or control.
- 2. The parties will supplement their disclosures in accordance with Fed. R. Civ. P. 26(e) with discoverable ESI responsive to a particular discovery request or mandatory disclosure where that data is created after a disclosure or response is made (unless excluded under Sections (D)(3) or (E)(1)-(2)).
- 3. Absent a showing of good cause by the requesting party, the following categories of ESI need not be preserved:
 - a. Deleted, slack, fragmented, or other data only accessible by forensics.
 - b. Random access memory (RAM), temporary files, or other ephemeral data that are 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. Data in metadata fields that are frequently updated automatically, such as last-opened dates (see also Section (E)(5)).
 - e. Back-up data that are duplicative of data that are more accessible elsewhere.
 - f. Server, system or network logs.
 - g. Data remaining from systems no longer in use that is unintelligible on the systems in use.
 - h. Electronic data (e.g., email, calendars, contact data, and notes) sent to or from mobile devices (e.g., iPhone, iPad, Android devices), provided that a copy of all such electronic data is automatically saved in real time elsewhere (such as on a server, laptop, desktop computer, or "cloud" storage).
 - i. Defendants' and Plaintiffs' text messages, mobile devices, personal home computers, and personal email accounts. Defendants and Plaintiffs will

7 8

10

11

12

13

14

15

16

17 18

19

20

21

22 23

24

25

26

ORDER REGARDING DISCOVERY OF ELECTRONICALLY STORED INFORMATION

(Case No. 2:22-CV-00910-RSM)

not be required to search custodians' or Plaintiffs' personal messages (i.e., text messages) and personal email if Defendants confirm that those systems are not used for Defendants' work purposes in relation to the subject matter of the Complaint and Defendants' defenses and if Plaintiffs confirm that those systems are not used in relation to the subject matter of the Complaint and Plaintiffs' claims.

Ε. Privilege

- 1. A producing party shall create a privilege log of all documents or categories thereof fully withheld from production on the basis of a privilege or protection, unless otherwise agreed or excepted by this Agreement and Order. Privilege logs shall include a unique identification number for each document and the basis for the claim (attorney-client privileged or work-product protection). Attorneys shall be identified as such, including whether the attorney is outside counsel or in-house counsel. For ESI, the privilege log may be generated using available metadata, including author/recipient or to/from/cc/bcc names; the subject matter or title; and date created. Should the available metadata and identification of attorneys provide insufficient information for the purpose of evaluating the privilege claim asserted, the producing party shall include such additional information as required by the Federal Rules of Civil Procedure. Privilege logs will be produced to all other parties no later than 30 days after delivering a production unless an earlier deadline is agreed to by the parties. Further, all privilege logs shall be delivered to all parties no later than 30 days before the deadline for filing motions related to discovery.
- 2. Redactions need not be logged so long as the basis for the redaction is clear on the face of the redacted document.
- 3. With respect to privileged or work-product information generated after the filing of their original complaints, parties are not required to include any such information in privilege logs.

8

10 11

12

13

14

15

16

17

18

19 20

21

22

23

24

25

26

ORDER REGARDING DISCOVERY OF ELECTRONICALLY STORED INFORMATION

(Case No. 2:22-CV-00910-RSM)

- 4. Activities undertaken in compliance with the duty to preserve information are protected from disclosure and discovery under Fed. R. Civ. P. 26(b)(3)(A) and (B).
- 5. Pursuant to Fed. R. Evid. 502(d), the production of any documents, electronically stored information (ESI) or information, whether inadvertent or otherwise, in this proceeding shall not, for the purposes of this proceeding or any other federal or state proceeding, constitute a waiver by the producing party of any privilege applicable to those documents, including the attorney-client privilege, attorney work-product protection, or any other privilege or protection recognized by law. This Order shall be interpreted to provide the maximum protection allowed by Fed. R. Evid. 502(d). The provisions of Fed. R. Evid. 502(b) do not apply. Nothing contained herein is intended to or shall serve to limit a party's right to conduct a review of documents, ESI or information (including metadata) for relevance, responsiveness and/or segregation of privileged and/or protected information before production. Information produced in discovery that is protected as privileged or work product shall be immediately returned to the producing party.

Non-Party Discovery F.

- 1. A party that issues a non-party subpoena (the "issuing party") shall include a copy of this Agreement Regarding Discovery of Electronically Stored Information with the subpoena.
- 2. The issuing party shall be responsible for producing any documents obtained under a subpoena to all other parties.
- 3. If the non-party production is not Bates-stamped, the issuing party shall endorse the non-party production with unique prefixes and Bates numbers prior to producing them to all other parties.

1	ORDER
2	IT IS SO ORDERED.
3	
4	DATED: November 22, 2024
5	
6	RICARDO S. MARTINEZ
7	UNITED STATES DISTRICT JUDGE
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	ORDER REGARDING DISCOVERY OF ELECTRONICALLY STORED INFORMATION PAGE - 10

(Case No. 2:22-CV-00910-RSM)

26