UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT _____

[PLAINTIFF],
 	
                    Plaintiff,
 	
          v.
 	
[DEFENDANT],
 	
                    Defendant.
	CASE NO. [CASE #]
	
	[MODEL] AGREEMENT REGARDING DISCOVERY OF ELECTRONICALLY STORED INFORMATION AND [PROPOSED] ORDER

[The red/italicized portions set forth guidance and instruction to the parties in formulating their agreement and should be deleted from the text of the final agreement. Optional provisions may be useful in cases involving more complicated ESI issues or productions.]

The parties hereby stipulate to the following provisions regarding the discovery of electronically stored information ("ESI") in this matter:

A.   General Principles

1.   An attorney's zealous representation of a client is not compromised by conducting discovery in a cooperative manner. The failure of counsel or the parties to litigation to cooperate in facilitating and reasonably limiting discovery requests and responses raises litigation costs and contributes to the risk of sanctions.

1   2.   As provided in LCR 26(f), the proportionality standard set forth in Fed. R. Civ. P.

2   26(b)(1) must be applied in each case when formulating a discovery plan. To further the

3   application of the proportionality standard in discovery, requests for production of ESI and related

4   responses should be reasonably targeted, clear, and as specific as possible. This agreement is

5   intended to assist the parties in identifying relevant, responsive information that has been stored

6   electronically and is proportional to the needs of the case. The agreement does not supplant the

7   parties' obligations to comply with Fed. R. Civ. P. 34.

8   **B.   ESI Disclosures**

9   Within 30 days of entry of this Order, or at a later time if agreed to by the parties, each

10   party shall disclose:

11   1.   <u>Custodians.</u> The custodians most likely to have discoverable ESI in their

12   possession, custody, or control. The custodians shall be identified by name, title, connection to

13   the instant litigation, and the type of the information under the custodian's control. *The parties*

14   *are expected to meet and confer to establish the appropriate number of custodians to be disclosed*

15   *based on the complexity, proportionality and nature of the case. Disputes should promptly be*

16   *submitted to the Court for resolution. This disclosure provision is distinct from the parties'*

17   *agreement set forth in Section C below about determining the number of custodians from whom*

18   *ESI should be gathered.*]

19   2.   <u>Non-custodial Data Sources.</u> A list of non-custodial data sources (*e.g.*, shared

20   drives, servers), if any, likely to contain discoverable ESI. [*These lists can identify the*

21   *databases that are likely to contain discoverable structured data.*]

22   3.   <u>Third-Party Data Sources.</u> A list of third-party data sources, if any, likely to

23   contain discoverable ESI (*e.g.*, third-party email providers, mobile device providers, cloud

24

25   AGREEMENT REGARDING DISCOVERY OF ELECTRONICALLY
     STORED INFORMATION AND [PROPOSED] ORDER   PAGE - 2
26   (Case No. [CASE #])

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).

[Section (D)(3) below sets forth data sources and ESI which are not required to be preserved by

the parties. Those data sources and ESI do not need to be included on this list.]

5. [*Optional*] <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 any

ESI or other discovery request.

C.   ESI Discovery Procedures

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 Court presumes that the use of search terms and*

queries, file type and date restrictions, and technology-assisted review will be reasonably

necessary to locate or filter some ESI likely to contain discoverable information. The timelines

and search related numbers in this section may be sufficient in certain cases, but not in others.

The parties are expected to meet and confer to establish the appropriate timing and terms based

on the complexity, proportionality and nature of the case.] 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.

    ii.   After disclosure, the parties will engage in a meet and confer process regarding additional terms sought by the non-producing party.

    iii.   The following provisions apply to search terms / queries of the 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 multiple words or phrases (*e.g.*, "computer" and "system") narrows the search and shall count as a single search term. A disjunctive combination of multiple words or phrases (*e.g.*, "computer" or "system") broadens the search, and thus each word or phrase shall count as a separate search 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. .

    c.   [*Optional*] 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

1   personnel, or the backup and systems recovery routines, including, but not limited to, tape

2   rotation and destruction/overwrite policy.

3   3.   Format.

4   a.   ESI will be produced to the requesting party with searchable text, in a

5   format to be decided between the parties. Acceptable formats include, but are not limited to, native

6   files, multi-page TIFFs (with a companion OCR or extracted text file), single-page TIFFs (only

7   with load files for e-discovery software that includes metadata fields identifying natural document

8   breaks and also includes companion OCR and/or extracted text files), and searchable PDF.

9   b.   Unless otherwise agreed to by the parties, files that are not easily converted

10   to image format, such as spreadsheet, database, and drawing files, will be produced in native

11   format.

12   c.   Each document image file shall be named with a unique number (Bates

13   Number). File names should not be more than twenty characters long or contain spaces. When a

14   text-searchable image file is produced, the producing party must preserve the integrity of the

15   underlying ESI, *i.e.*, the original formatting, the metadata (as noted below) and, where applicable,

16   the revision history.

17   d.   If a document is more than one page, the unitization of the document and

18   any attachments and/or affixed notes shall be maintained as they existed in the original document.

19   e.   [*Optional*] The parties shall produce their information in the following

20   format: single- page images and associated multi-page text files containing extracted text or with

21   appropriate software load files containing all information required by the litigation support system

22   used by the receiving party.

23

24

25   AGREEMENT REGARDING DISCOVERY OF ELECTRONICALLY
     STORED INFORMATION AND [PROPOSED] ORDER   PAGE - 5
26   (Case No. [CASE #])

f. [*Optional*] 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).

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 tracked in a duplicate/other custodian field in the database load file.

5. <u>Email Threading.</u> 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. Upon reasonable request, the producing party will produce a less inclusive copy.

6. <u>Metadata fields.</u> 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 in light of advances and changes in technology, vendor, and business practices.

7. [*Optional*] <u>Hard-Copy Documents.</u> 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 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).

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).

[The parties should confer regarding any other categories of ESI that may not need to be preserved, such as text messages and social media data, in light of the General Principles set forth above, and determine whether they can agree that such categories can be added to the non-preservation list above.]

E.   Privilege

[The parties should confer regarding the nature and scope of privilege logs for the case, including whether categories of information may be excluded from any logging requirements and whether alternatives to document-by-document logs can be exchanged.]

1.   A producing party shall create a privilege log of all documents 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). 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 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 [*alternative language, choose one of the following clauses*] [*alternative 1*] [no later than 30 days after delivering a production] [*alternative 2*] [no later than 30 days before the deadline for filing motions related to discovery] unless an earlier deadline is agreed to by the parties.

2.   Redactions need not be logged so long as the basis for the redaction is clear on the redacted document.

3.   With respect to privileged or work-product information generated after the filing of the complaint, parties are not required to include any such information in privilege logs.

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.

DATED: _____

[Signature blocks]

ORDER

Based on the foregoing, IT IS SO ORDERED.

DATED: _____

_____
The Honorable _____
UNITED STATES DISTRICT JUDGE