

## **GUIDELINES FOR USE OF THE MODEL AGREEMENT REGARDING DISCOVERY OF ELECTRONICALLY STORED INFORMATION**

Experience increasingly demonstrates that discovery of electronically stored information (“ESI”) poses challenges for litigants (both parties and their attorneys) and for courts beyond the issues typically encountered and addressed when dealing with discovery of traditional, hard-copy documents. The United States District Court for the Western District of Washington recognizes that ESI is now frequently the subject of discovery and that such discovery can be extremely burdensome, time-consuming, and expensive. The Court believes that establishing a framework for anticipating and addressing ESI-related discovery at the earliest stages of litigation will encourage mutual and cost-effective solutions and speedier and more informed resolution of disputes.

In furtherance of these goals, the Court has developed the Model Agreement Regarding Discovery of Electronically Stored Information (“Model ESI Agreement”) set forth below. The Model ESI Agreement sets forth the general principles and basic provisions that the Court expects will apply in most cases involving ESI discovery, and is intended to serve as a framework for addressing and resolving a wide range of ESI issues. The Model ESI Agreement is intended to be a flexible checklist, and not all aspects of it may be applicable or practical for a particular matter. The Model ESI Agreement may be adopted in its entirety by the parties without any changes, or it may be adapted, as appropriate. The Court has also included additional provisions that may be appropriate and useful in addressing more complicated ESI discovery issues. These additional provisions follow the text of the Model ESI Agreement below.

The Court expects that the parties will consider the nature of the claim, the amount in controversy, agreements of the parties, the relative ability of the parties to conduct discovery of ESI, and such other factors as may be relevant under the circumstances in deciding on adopting and/or tailoring the provisions of the Model ESI Agreement. The Court encourages the parties to use the Model ESI Agreement in cases in which there will be discovery of ESI and to resolve ESI issues informally, early, and without Court supervision whenever possible.



2. Non-custodial Data Sources. A list of non-custodial data sources (e.g. shared drives, servers, etc.), if any, likely to contain discoverable ESI.

3. Third-Party Data Sources. A list of third-party data sources, if any, likely to contain discoverable ESI (e.g. third-party email and/or mobile device providers, “cloud” storage, etc.) 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. Inaccessible Data. 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)(C)(i). [*Section (C)(2)(a)(i) 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.*]

### **C. Preservation of ESI**

The parties acknowledge that they have a common law obligation 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. All parties shall supplement their disclosures in accordance with Rule 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 (C)(2) or (D)(1)-(2) below).

2. 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 substantially 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, and Blackberry devices), *provided* that a copy of all such electronic data is routinely saved 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.]*

#### **D. 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. 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.

2. 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).

3. Information produced in discovery that is protected as privileged or work product shall be immediately returned to the producing party, and its production shall not constitute a waiver of such protection, if: (i) such information appears on its face to have been inadvertently produced or (ii) the producing party provides notice within 15 days of discovery by the

producing party of the inadvertent production.

#### **E. ESI Discovery Procedures**

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

2. Search methodology. [*The Court presumes that in the majority of cases, the use of search terms will be reasonably necessary to locate or filter ESI likely to contain discoverable information.*] The parties shall attempt to reach agreement on appropriate search terms, or an appropriate computer- or technology-aided methodology, before any such effort is undertaken. The parties shall continue to cooperate in revising the appropriateness of the search terms or computer- or technology-aided methodology.

a. A producing party shall disclose what search terms, if any, were used to locate ESI likely to contain discoverable information. If search terms were not used, the producing party shall disclose the search methodology used to locate ESI likely to contain discoverable information.

b. If search terms were used to locate ESI likely to contain discoverable information, a requesting party is entitled to no more than 5 additional terms or queries to be used in connection with further electronic searches absent a showing of good cause or agreement of the parties. The parties shall confer in good faith on the 5 additional terms or queries. Focused terms and queries, rather than overbroad ones (e.g., product and company names), should be employed.

c. Absent a showing of good cause, search terms returning more than 250 megabytes of data are presumed to be overbroad.

d. The producing party shall search both non-custodial data sources and ESI maintained by the custodians identified above.

3. Format. The parties agree that 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, TIFF (with a companion text file), and searchable PDF. Unless otherwise agreed to by the parties, files that are not easily converted to image format, such as spreadsheet, database and drawing files, should be produced in native format.

4. De-duplication. The parties may de-duplicate their ESI production across custodial and non-custodial data sources after disclosure to the requesting party.

5. Metadata fields. If the requesting party seeks metadata, the parties agree that only the following metadata fields need be produced: document type; custodian and duplicate custodians; author/from; recipient/to, cc and bcc; title/subject; file name and size; original file path; date and time created, sent, modified and/or received; and hash value.

DATED: \_\_\_\_\_

PARTY 1

PARTY 2

By \_\_\_\_\_

By \_\_\_\_\_

**ORDER**

Based on the foregoing, IT IS SO ORDERED.

DATED: \_\_\_\_\_

\_\_\_\_\_  
The Honorable \_\_\_\_\_  
United States District Court Judge

## **ADDITIONAL PROVISIONS FOR MORE COMPLEX CASES**

In addition to the provisions set forth in the Model ESI Agreement above, parties may find the following provisions appropriate and useful in addressing more complicated ESI discovery issues. The complexity of ESI discovery varies from case to case and is not necessarily tied to the number or size of the parties or the amount in controversy. The additional provisions below are intended to assist parties in anticipating and addressing early on more complicated ESI discovery issues but may not be appropriate or necessary in every case. The following provisions are intended as suggested provisions from which parties may pick and choose, taking into consideration the needs of the particular case.

1. Search methodology.

Upon reasonable request and if appropriate for the particular case, a party shall also 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.

2. Format.

a. Each document image file shall be named with a unique Bates Number (e.g. the unique Bates Number of the page of the document in question, followed by its file extension). 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 preserve the integrity of the underlying ESI, i.e., the original formatting, the metadata (as noted below) and, where applicable, the revision history. The parties shall produce their information in the following format: single-page images and associated multi-page text files containing extracted text or with appropriate software load files containing all requisite information for use with the document management system (e.g., Concordance® or Summation®), as agreed to by the parties.

b. If appropriate to the particular case, the parties shall consider whether or not the full text of each electronic document shall be extracted ("Extracted Text") and produced in a text file. If the parties so agree, 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).

c. 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.

3. Metadata fields. The parties are to confer and agree on whether metadata is to be produced or may be excluded from discovery. Metadata may not be relevant to the issues presented or, if relevant, may not be reasonably subject to discovery, or may be subject to cost-shifting, considering the cost-benefit factors set forth in Fed. R. Civ. P. 26(b)(2)(C). For example, if one party is producing only paper documents, and the other party is producing ESI, the parties should confer on whether the additional cost and burden of producing metadata by the party producing ESI is reasonable or should be shifted under the facts and circumstances of the case. If the parties agree to produce metadata, and unless otherwise agreed, each party shall produce the following metadata associated with ESI to the extent reasonably accessible: (a) the author(s) of the ESI; (b) the recipient(s) of the ESI; (c) the date the ESI was created; and (d) the source from which the ESI was produced. The "source" of ESI shall be the name of the person who was the custodian of the ESI or, if the name of a person is not available, the storage location (e.g., "Regulatory Shared Drive-Wayne, PA"). This information will be included in the "Author," "Recipient," "Date," and "Source" fields (respectively) for each document in the load file associated with the document images. Although it is presumed generally that the above list of metadata fields will be provided, the list of metadata fields 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.

4. Hard-Copy Documents. If the parties elect to produce hard-copy documents in an electronic format, the production of hard-copy documents shall include a cross-reference file that indicates document breaks and sets forth the Custodian or Source associated with each produced document. Hard-copy documents shall be scanned using Optical Character Recognition technology and searchable ASCII text files shall 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 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).