

Exhibit A

Case Management Statement Exhibit A – Electronic Discovery Protocol

1. **Preservation.** The Parties acknowledge and agree to abide by their respective obligations to take reasonable steps to preserve discoverable documents and things in their possession, custody, or control.

a. Absent a showing of good cause by the requesting party, the Parties shall not be required to modify, on a going-forward basis, the procedures used by them in the ordinary course of business to back up or archive data; provided, however, that the Parties shall preserve the non-duplicative discoverable information currently in their possession, custody, or control.

b. Absent a showing of good cause by the requesting party, the following categories of ESI need not be preserved, restored, collected, or produced:

1. deleted, slack, fragmented, unallocated, or other data only accessible by forensics;
2. random access memory (RAM), temporary files, or other ephemeral data that is difficult to preserve without disabling the operating system;
3. on-line access data such as temporary internet files, history, caches, cookies, and the like;
4. data in metadata fields that are frequently updated automatically, such as last-opened dates;
5. archival or disaster recovery back-up data;
6. voice and text messages;
7. instant messages that are not ordinarily printed or maintained in a server dedicated to instant messaging;
8. electronic data (*e.g.* e-mail, calendars, contact data, notes, and text messages) sent to or from mobile devices (*e.g.* iPads or other tablets and iPhones or other “smart” phones), provided that a copy of all such data is routinely saved elsewhere (such as on a server, laptop, desktop computer, or “cloud” storage);
9. server, system, or network logs;
10. electronic data temporarily stored by laboratory equipment or attached electronic equipment, provided that such data is not ordinarily preserved as a part of a laboratory report;
11. data remaining from legacy systems no longer in use that is unintelligible on the system now in use; and
12. social media pages or commentary.

2. **Collection and Production.** Each party shall be responsible for generating a searching protocol that it believes in good faith will return a reasonably high proportion of documents and things responsive to each party’s requests for production. Each Party shall disclose its above-described searching protocol to all other parties in this case upon request; that is, each Party’s respective searching protocol or methodology is not protected from discovery by the attorney-client privilege or the work product doctrine. The Parties agree to work together with respect to requests for reasonable modifications or additions to their respective searching protocol or methodology. Consistent with this paragraph, the Parties may reach agreement on the scope of

and procedure for their respective document collection and production, in lieu of serving formal requests for production under Rule 34.

3. Production Format. The Parties agree to produce ESI in the following format in line with Federal Rule of Civil Procedure 34(b)(1)(C):

a. at the producing party's option, either native files or single page Group IV TIFF files imaged to at least 300 dpi, with each image endorsed with a Bates number;

b. load files that map to all of the TIFF images and depict the document boundaries and attachment (parent/child) relationships (if a document is more than one page, the unitization of the document and any attachments shall be maintained as they existed in the original document) and;

c. such data load files which contain extracted text and available metadata fields corresponding to those listed below (to the extent such fields exist and are available):

<u>Metadata Fields:</u>	<u>Description</u>
BegDoc#	The bates label of the first page of the document
EndDoc#	The bates label of the last page of the document
To	The recipient of the document or email
From	The author of the document or email
CC	Persons copied on the document or email
BCC	The persons blind-copied on the document or email
Custodian	The person who maintains custody of the document or email
Date Created	Document date or date email was created
Date Sent	Date document or email was sent
Date Received	Date document or email received by recipient
Date Last Modified	Date last modified for attachments and standalone electronic files
Date Last Printed	Date last printed for attachments and standalone electronic files
Email Subject	Subject of email
Doc Title	Title of document
File Name	File name of electronic document
File Path	File path as maintained by operating system
Folder	Email folder information
Attachment ID	Bates range of document or email attachment
Parent ID	Bates range of parent document or email
MD5 Hash	

d. All spreadsheets (*e.g.* Excel files), presentations (*e.g.* PowerPoint files), database files, graphics, audio files, video files, animations, and other files that cannot readily be converted to TIFF format or that reasonably require access to the native file, shall be produced in native format with all metadata intact (and not as a TXT file).

e. The Parties will produce additional native files and accompanying metadata in response to reasonable requests. The Parties will make reasonable efforts to ensure that all documents produced in native form are decrypted, but the Parties have no duty to identify encrypted documents prior to production.

f. The Parties will make reasonable efforts to agree upon the format for producing data from a structured database using existing report formats or report formats that can be developed without undue burden.

g. Web pages, social media data, and other information not otherwise covered above shall be produced as “screen shots” or in native format.

h. Documents originally maintained in paper or other non-electronic format and documents not searchable in their native format shall be produced as TIFF files endorsed with a bates number with their contents in a single TXT file (not one TXT file per page) using optical character recognition (OCR) and a load file that maps the TXT file to the corresponding TIFF file. Any redacted or privileged material should be labeled clearly to show the redactions.

i. In scanning paper documents, distinct documents should not be merged into a single record, and single documents should not be split into multiple records. That is, paper documents should be logically unitized. In the case of an organized compilation of separate documents – *e.g.*, a binder or file folder containing several separate documents behind tabs of sub-files – the document behind each tab or sub-file should be scanned separately, but the relationship among the documents in the compilation should be reflected in the proper coding of the beginning and ending document and attachment fields. The Parties will use their best efforts to unitize the documents correctly. (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, folders, binders, and other logical indicators.)

4. **De-duplication.** A party is only required to produce a single copy of a responsive document. The Parties may de-duplicate stand-alone documents or entire document families using MD5 or SHA-1 Hash value matching. (Common system files defined by the NIST library (<http://www.nsl.nist.gov/>) need not be produced.) However, (i) attachments to e-mails shall not be eliminated from the parent e-mail, and (ii) paper documents shall not be eliminated as duplicates of responsive ESI. To the extent the parties de-duplicate stand-alone electronic documents against an e-mail attachment, the attachment to the e-mail must be the document that is produced. ESI that is not an exact duplicate may not be removed.