Lexbe Sample ESI Discovery Protocol[1]

This stipulated agreement[2] regarding discovery and production of electronically stored information ("ESI Discovery Protocol") governs discovery of electronically stored information ("ESI") in this case. Consistent with the provisions of this ESI Discovery Protocol, each party shall preserve, collect and produce responsive ESI to other party or parties as provided herein.

1. ESI to be Preserved. A party is obliged to consider for preservation, identification and production all potentially responsive information items and data sources over which the party (including its employees, officers and directors) has possession, physical custody or a right or ability to exert direction or control, so long as reasonable and proportionate. Preservation obligations include the metadata specified in Appendix A when available. The belief that an employee, agent or contractor may fail to act upon or conform to an attempted exercise of direction or control is not a justification for any party to fail to undertake an exercise of direction or control directed to preservation, identification and, as potentially responsive or relevant, production of information items and data sources.

2. ESI that Need not be Preserved. Absent a showing of good cause by a requesting party, the following categories of ESI need not be preserved:

a) Deleted, slack, fragmented, or other data only accessible by forensics.

b) Server, system or network logs.

c) Random access memory (RAM), temporary files, or other ephemeral data that are difficult to preserve without disabling the operating system.

d) On-line access data such as temporary internet files, history, cache, cookies, and the like.

e) Back-up data that are substantially duplicative of data that are more accessible elsewhere.

f) ESI remaining from systems no longer in use that is unintelligible on the systems in use.

g) ESI sent to or from mobile devices provided a copy of that data is routinely saved elsewhere.

h) ESI stored on photocopiers, scanners, and fax machines.

i) ESI 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).

j) Data stored in a backup system for the purpose of system recovery or information restoration, including but not limited to, disaster recovery backup tapes, continuity of operations systems, data or system mirrors or shadows unless it is the only known source of potentially relevant data.

Nothing in this section or Protocol shall relieve a party from their obligation to preserve data sources accessed in the ordinary course of business, including disaster recovery media and systems used for

---

[1] This sample form is provided as a courtesy by Lexbe for use by experienced attorneys AS IS, and should be customized for the particular jurisdiction, case, court and circumstances. In particular, some optional or alternative options are offered in yellow highlighting. For background, see our Webinar: Negotiating a State of the Art eDiscovery protocol, available on demand at the Lexbe website. If you have any questions or comments, or would like specific consultation, please contact us.

Some provisions in this Protocol might alternately be addressed in a Case Management Order or in a Protective Order. Some courts have standard ESI Protocols which must be used in cases in their jurisdiction in general or in particular case types.

[2] The protocol can be implemented as an agreement between litigants, as an agreed order, or as a non-agreed order as a result of a hearing, with appropriate modifications.

archival purposes where such data source is the unique source of that data.

3. ESI Not Reasonably Accessible.

a) The parties have taken or will take reasonable steps to collect potentially relevant ESI stored on servers, workstations and readily accessible drives. The parties shall discuss sources of potentially relevant information deemed "not reasonably accessible."

b) If either party objects to producing the requested information on the grounds that such information is not reasonably accessible because of undue burden or cost, or because production in the requested format is asserted to be not reasonably accessible because of undue burden or cost, and before asserting such an objection, the responding party will inform the requesting party of the format in which it is willing to produce it, the nature and location of the information claimed to not be reasonably accessible, the reason(s) why the requested form of production would impose an undue burden or is unreasonably costly, and afford the requesting party notice to propose an alternative means of compliance with the request. Such proposal may include alternative cost estimates for ESI discovery production.

(c) When a party seeks production of information from sources designated by another party as "not reasonably accessible," the parties shall meet and confer in an effort to resolve any disagreements before seeking relief from the Court.

(d) The parties agree that these data sources are not reasonably accessible because of undue burden or cost and ESI from these sources will be preserved but not searched, reviewed, or produced: [e.g., backup media of [named] system, systems no longer in use that cannot be accessed].

(e) Among the sources of data the parties agree are not reasonably accessible, the parties agree not to preserve the following: [e.g., backup media created before _____, digital voicemail, instant messaging, automatically saved versions of documents].

4. Data Mapping & Information Exchange. The parties agree to exchange in writing the information listed in items (a) through (e) below. The parties agree and understand that their respective responses are based on their knowledge and understanding as of the date of the response, and each party agrees to amend or supplement its responses in a timely manner if it learns that in some material respect its response is incomplete or incorrect.

a) A list of custodians (including current employees, former employees and any other individuals or companies) likely to have discoverable information, including job title and a brief description of job responsibilities and employment period for each individual to the extent that it exists and is reasonably accessible.

b) A general description of systems for electronic communications and ESI storage likely to contain discoverable information (e.g. shared network storage and shared electronic work spaces).

c) For databases identified, the producing party should provide the following information (to the extent that it is reasonably available): Database name, type of database software platform, software version, business purpose, a list of existing relevant reports used in the ordinary course of business, database owner/administrator, database field list within the scope of permissible discovery. As needed,

the parties will meet and confer to discuss reports and fields within the scope of permissible discovery.

d) A general description or, at the producing party's option, copies of the party's operative document retention policies, throughout the relevant time period, pertaining to known data within the scope of discovery.

e) If unique, non-duplicative ESI within the scope of discovery is lost or destroyed after the legal hold obligations have been triggered in this case, if known.

f) A description of any ESI within the scope of discovery that the producing party contends is inaccessible or only of limited accessibility and, hence, not producible by that party without undue burden and/or expense, including: (1) The reasons for the Party's contention regarding accessibility; and (2) The proposed capture and retrieval process available (if any) for identification and/or recovery of the information deemed inaccessible (including cost estimates if readily available).

5. Custodian Collection Procedures.[3] For each of a producing party's current or former employees identified as a custodian in the matter, the producing party will do the following:

a) Unless a producing party establishes good cause to the contrary, a producing party will collect all emails sent to or received by a custodian regardless of whether such emails are in the custodian's actual email account.

b) Data from current or previous mobile, cell or smartphone devices during the relevant time periods of the matter will be preserved by direct device collection using an industry standard collection tool for each custodian, including without limitation text messaging.

c) Provide a list of every personal computer or similar device used by the custodian during the relevant periods of the matter, the model number of the personal computer, the present physical location of the computer, any backups that exist of the information from such a personal computer, and if a personal computer used by a custodian has been lost or destroyed, provide the date upon which it was lost or destroyed. A producing party will also identify whether any backups for other devices, exist for the personal computer.

d) Identify any tablet computers, smartphones, or other mobile phones used by a custodian during the relevant periods of the matter.

e) To the extent a custodian made any use of cloud-based document storage services (such as Apple iCloud, Google, Amazon, Box, DropBox, Microsoft, etc.) for work-related purposes, a producing party will obtain such information and produce responsive information. To the extent a custodian backed up a computer, mobile phone or tablet to a cloud-based storage system, a producing party will obtain such information and produce responsive information. If for some reason a producing party is unable to obtain cloud-based ESI for a custodian, then a producing party will provide the requesting party with a written explanation of the circumstances of the inability, including (i) the name of the custodian, (ii) the name of the cloud-based system on which the data is believed to be stored, (iii) a description of the type of ESI

[3] This provision could be expanded or reduced depending on the particularities of the organization and litigation.

believed to be stored in the Cloud-based system, (iv) the efforts a producing party undertook to obtain the information, (v) whether any data on the cloud-based email system is believed to have been deleted or lost, and if so, when, and (vi) whether or not the user name and password for such information is known to the custodian and/or producing party.

f) If a custodian used organizational chat or messaging applications (e.g., Skype, Slack, Salesforce, Teams, etc.) or personal chat or messaging applications (e.g., Facebook, WhatsApp, Viber, Snapchat, Hangouts, Messenger) for work-related purposes, a producing party will obtain such information and produce responsive information. If for some reason a producing party is unable to obtain chat and messaging ESI for a custodian, then a producing party will provide the requesting party with a written explanation of the circumstances of the inability, including (i) the name of the custodian, (ii) the name of the chat or messaging system on which the data is believed to be stored, (iii) a description of the type of ESI believed to be stored in the messaging or chat application, (iv) the efforts a producing party undertook to obtain the information, (v) whether any data on the messaging or chat application is believed to have been deleted or lost, and if so, when, and (vi) whether or not the user name and password for such information is known to the custodian and/or producing party.

g) Provide a custodian's contacts (e.g., MS Outlook Contacts, phone-based contacts, email based contacts will be exported to MS Excel or CSV) from the custodian's email account and/or phone with all available metadata fields included in the extraction. If a producing party desires to redact certain personal information (e.g., phone numbers for a custodian's children), then the parties will meet and confer regarding the categories of such information to be redacted and how such information will be redacted and/or excluded from MS Excel (or CSV).

h) Unless otherwise agreed, an agreement to produce documents for a particular custodian shall include the collection of that custodian's current and/or former administrative assistants or secretaries.

6. Processing. The parties may apply the following standard procedures as part of ESI processing:

a) ESI may be de-NISTed using the industry standard list of such files maintained in the National Software Reference Library by the National Institute of Standards & Technology. Other file types may be added to the list of excluded files by agreement of the parties.

b) ESI items shall be processed in a manner that preserves their existing time, date, and time-zone metadata (e.g., the email of a Document Custodian located in Texas will be processed as Central Time, while a custodian located in California will be processed as Pacific Time). If GMT time zone is used instead, the producing party will provide the original time zone in which the custodian of the document received or authored the document, or if not available, the usual time zone of the custodian.

c) ESI items shall be processed so as to preserve the date/time shown in the document as it was last saved, to the extent reasonably available, not the date of collection or processing.

d) The parties agree to provide the metadata fields for all ESI produced, to the extent such metadata exists, as described in Appendix A.

e) A party is only required to produce a single copy of a responsive document per custodian. Parties may de-duplicate stand-alone documents or entire document families using hash value matching

(such as MD5 or SHA-1 values). ESI that is not an exact duplicate may not be removed. Partial email families may not be removed. Paper documents shall not be eliminated as duplicates of responsive ESI. If a producing party elects to de-duplicate horizontally, all custodians who were in possession of a de-duplicated document must be identified in a metadata field as part of the loadfile or a subsequent overlay file.

OPTION 1 - NO AGREED SEARCH TERMS

7. Use of Search Terms for Document Review. The parties agree to meet and confer about the methods they will use to search ESI to identify information that is subject to production, and cull or filter out ESI that is not subject to discovery. The parties will cooperate in the development of appropriate search methodology and criteria, including the potential use of computer-assisted search methodologies and other analytics-based search and filtering tools.

OPTION 2 - AGREED SEARCH TERMS

7. Use of Search Terms for Document Review. Within twenty-one days of a party's response, the producing party will provide the receiving party with an initial listing of search terms and the receiving party shall have the opportunity to propose modifications to those search terms. Either party may also propose custodians and date limitations for searches. Within ninety days of when the parties agree on an initial set of search terms, the parties shall conduct a meet and confer to determine whether modifications should be made to those search terms. The parties will produce potentially-relevant ESI in their possession according to the agreed search terms, custodians and date ranges. Each party shall be provided with an opportunity to propose additions or amendments to the search procedures and terms. The parties acknowledge that the agreement to the use of such search procedures and terms shall not be construed as a waiver of any party's right to request subsequent searches and productions, particularly where there is a showing that the agreed-to search terms and procedures have resulted in inadequate productions or failed to identify relevant materials. The parties reserve their right to object to any additional requests or subsequent searches.

8. Technology Assisted Review. Prior to using predictive coding/technology assisted review (TAR) for the purpose of identifying or culling the documents to be reviewed or produced, the producing party will notify the requesting party with ample time to meet and confer in good faith regarding a mutually agreeable protocol for the use of such technologies or alternatives. While no specific benchmarks or stabilization percentages are available prior to undertaking TAR processes, a producing party has an obligation to make their best efforts to ensure that the process meets a Rule 26(g) standard. The parties will be transparent in the TAR technology and vendor used, and will meet and confer as needed. Transparency will include, at minimum: a) the TAR algorithm used, b) if applicable, the seed set size and contents, c) how the seed set was chosen, d) the control set size, if applicable, the F score (precision and recall).

9. Databases. To the extent a response to discovery requires production of discoverable electronic information contained in a database, in lieu of producing the database, the parties shall meet and confer to, with an understanding of which fields are relevant, agree upon a set of queries to be made for relevant reports used in the ordinary course of business and other discoverable information and generate a report in a reasonably usable and exportable electronic file (e.g., Excel or CSV format) for review by the

requesting party or counsel. Upon review of the report(s), the requesting party may make reasonable requests for additional information to explain the database schema, codes, abbreviations, and different report formats or to request specific data from identified fields.

9. Paginated Versions of Documents. All documents to be produced will be converted to a paginated version as a PDF and/or TIFF images ("Paginated Document"), as provided in this section:

(a) Produced PDFs will be in the form of one PDF file per document, multi-page as applicable (Produced PDFs). A PDF produced as a Paginated Document will not be encrypted or otherwise include settings to impair searchability, copying or print. Embedded images will not be reduced or below 300 dpi.

(b) TIFF images produced as Paginated Documents will be in the form of single-page Tagged Image File Format images (Produced TIFFs) and shall be saved and produced in the Group 4 compression single-page TIFF format. Each of the Produced TIFF files will be accompanied with a corresponding text file containing extracted or OCR text.

(c) All Produced PDFs and Produced TIFFs generated from hard copy documents shall be scanned as 300 dpi resolution.

(d) All Paginated Documents shall reflect to the extent practicable, without visual degradation, the full and complete information contained on the original document.

(e) A PDF or TIFF placeholder will be generated for any file that cannot be converted as a Paginated Document. In each case, a corresponding native document will be produced, subject to withholding for privilege or work-product.

(f) Documents that contain color in a manner material to the meaning or understanding of the document, shall be produced as a Paginated Document in color. If a party is producing Paginated Documents as Produced PDFs, then the Produced PDF conversion settings will include settings that preserve color to the extent practicable. If a party is producing Paginated Documents as Produced TIFFs, then the producing party shall also produce color PDFs for such Paginated Documents, or substitute color PNG or JPG images for TIFF Images.

(g) A Paginated Document may truncate pagination after a limit of at least 100 pages. In such cases the native version will be made available, subject to redaction limitations.

10. Redactions.

a) Files that must be redacted pursuant to any applicable protective order or applicable law, should be produced as Produced PDFs or Produced TIFFs in redacted form, with applicable TIFF text files or PDF text layers, containing extracted or OCRed text acquired after redaction.

b) Native documents corresponding with redacted documents may be withheld from production, or a party may employ native redaction techniques so long as the method of redaction employed does not significantly impair the usability or searchability of the redacted item and the fact of alteration is disclosed.

c) Redactions must be logged in the manner of any other responsive material withheld on claims of privilege.

d) If the items redacted and partially withheld from production are PowerPoint-type presentation decks or Excel-type spreadsheets, and the native versions are also withheld, then the entire Paginated Document must be produced as a Produced PDF or Produced TIFF, including all unprivileged pages, hidden fields and other information that does not print when opened as last saved by the custodian or end-user. For PowerPoint-type presentation decks, this shall include, but is not limited to, any speaker notes. For Excel-type spreadsheets, this shall include, but is not limited to, hidden rows and columns, all cell values, annotations and notes.

e) The producing party shall also make reasonable efforts on request to ensure that any spreadsheets produced only as Produced PDFs or Produced TIFFs are formatted so as to be legible. For example, column widths should be formatted so that the numbers in the column will display readable content rather than "##########."

f) If the items redacted and partially withheld from production are audio/visual files, the producing party shall provide the unredacted portions of the content. If the content is a voice recording, the parties shall meet and confer to discuss the appropriate manner for the producing party to produce the unredacted portion of the content.

h) A party may not make any redactions based upon the purported relevancy or non-relevancy of a document.

OPTION 1 - ALL NATIVES EXCEPT PRIVILEGED & REDACTED

11. Native Files. The parties will also produce native files corresponding with all produced documents, with the exception of native files that correspond to produced Paginated Documents that have been redacted, or native files that are containers of files (e.g., .Zip, .RAR, other archive files, or .msg, .pst or other email files) that contain privileged, work-product or redacted information.

OPTION 2 - ONLY SPREADSHEETS AND PRESENTATIONS

11. Native Files. The parties will not be required to produce native files corresponding with produced Paginated Documents, with the exception of spreadsheets (e.g. Excel), presentations (e.g., PowerPoint), databases or other documents that cannot be converted to a Paginated Document without material loss in data or presentation. A receiving party may request other native documents as needed, and supplemental production will not be unreasonably withheld. All documents that have not converted to a Paginated Document (e.g., placeholder files), shall be produced in native format unless they contain privileged, work-product or redacted information.

OPTION 3 - NO NATIVES EXCEPT WITH CAUSE

11. Native Files. The parties will not be required to produce native files corresponding with produced Paginated Documents, without a good cause showing. A receiving party may request native documents as needed, with reasons why the Paginated Document version does not provide adequate information. Any native documents so produced may be redacted as needed for PII or privilege using native redaction tools.

12. Parent-Child Relationships. Parent-child relationships (e.g., the association between emails and attachments) will be preserved. Email attachments will be consecutively produced with the parent email, and families associated using attachment range metadata as specified in Appendix A. If a scanned document is more than one page, the unitization of the document and any attachments shall be maintained as it existed in the original when creating the Paginated Document. For documents that contain affixed notes, the pages will be scanned both with and without the notes, and those pages will be treated as part of the same document. The relationship of documents in a document collection (e.g., cover letter and enclosures, email and attachments, binder containing multiple documents or other documents where a parent-child relationship exists between the documents) shall be maintained through the scanning or conversion process. If more than one level of parent-child relationship exists, documents will be kept in order, but all will be treated as children of the initial parent document.

13. Bates Numbering. All produced Paginated Documents will include a legible, unique page identifier ("Bates Number") electronically embossed onto each page at a location that is reasonably intended to not obliterate, conceal or interfere with any information from the Paginated Document. No other legend or stamp will be placed on the Paginated Document other than a confidentiality legend (where applicable), redactions (consistent with any other protective orders or applicable law), any applicable protective orders and, if desired by a party, a document control number separate from the Bates Number. With respect to the identification of files produced in their native format, the parties shall identify each file produced using the Bates Number as the name, and link in the applicable loadfile. Bates number must be unique across the entire document production, maintain a constant length (0-padded) across the entire production, contain no special characters or embedded spaces, and (4) be sequential within a given document. The Bates number must not obscure any part of an underlying Paginated Document. If the placement in the lower right-hand corner will result in obscuring the underlying Paginated Document, the Bates number should be placed as near to that position as possible while preserving the underlying Paginated Document.

14. File Naming Conventions. Each Produced PDF Paginated Document file will be named with the beginning Bates Number. Each Produced TIFF image and corresponding text file shall be named with the unique Bates Number of the page of document. In the event the Bates Number contains a symbol and/or character that cannot be included in a file name, the symbol and/or character will be omitted from the file name.

15. Load Files. The parties shall produce load files that are compatible with commercially acceptable standards, including a 'Concordance DAT/OPT' load file and a 'Summation DII' load file, to accompany the Paginated Documents. Each load file shall include metadata and other information about the Paginated Documents through a document management or litigation support database system, including the fields in Appendix A. The parties shall meet and confer to the extent reasonably necessary to facilitate the import and use of the produced materials with commercially available document management or litigation support software.

16. Extracted Text/OCRed Text. For produced documents that exist natively in electronic format that have not been redacted and that are produced as Paginated Documents, the parties shall produce extracted text files reflecting the full text that has been electronically extracted from the original, native electronic files. The parties will produce corresponding extracted text (for native files and/or optical character recognition ("OCR") text for TIFF or other images) files for all hard-copy documents and any electronic

documents produced. For Produced TIFFs, the OCR and extracted text files shall be produced in ASCII text format, and shall be included with the load files. These text files will be named with the unique Bates Number of the first page of the corresponding document followed by the extension ".txt." For Produced PDFs, extracted or OCRed text shall be embedded in the PDF file in an accessible text layer. The OCR and extracted text files shall be produced in a manner suitable for importing the information into commercially available document management or litigation support software.

17. Exception Files. The parties will make reasonable efforts to identify documents that cannot be processed or converted to a Paginated Document due to technical difficulties (such as corruption, password protection, digital rights management or proprietary software associated to the file) as exception files. Identified exception files will be identifiable by placeholder file and/or a log that includes each file's name, custodian and reason for the exception. The parties will make reasonable efforts to ensure that documents produced in native form are decrypted (or that passwords are supplied).

18. Translations of Produced Materials. For any foreign-language documents responsive to document requests that a party translated or translates into the English language using human translators for its own purposes, except to the extent such translation is protected by attorney-client or work-product privileges, the producing party shall produce the translation of the original document with the original. This provision will not apply to auto or machine translations.

19. Privileged Information.

a) Any document falling within the scope of any request for production or subpoena that is withheld on the basis of a claim of attorney-client privilege, work-product or any other claim of privilege or immunity from discovery shall be identified by the producing party in a privilege log, which the producing party shall produce in an electronic format that allows text searching and organization of data.

b) An email thread contained within a single document need only be recorded once on the producing party's privilege log, even if a privilege is asserted over multiple portions of the thread.

c) Privilege log identification is not required for communications exchanged between the producing party and their litigation counsel or among counsel for the producing party after the date of filing of this action.

d) For each document for which a producing party asserts that a privilege applies, the producing party must include in the privilege log the information required by Federal Rule of Civil Procedure 26 (b)(5), including the following: (a) a statement of the ground(s) alleged for withholding such document; (b) the date of the document or communication; (c) the identity of its author and signatories and to whom it was sent; (d) whether the asserted privilege(s) also apply to any attachments; (e) an indication of all authors, signatories or recipients of the document who are attorneys; (f) a statement as to whether the entire document has been redacted/withheld or only a portion has been redacted, and the Bates number of the redacted document; and (g) a description of the withheld document, communication or tangible thing in a manner that, without revealing information claimed privileged or protected, will enable a party to assess the validity or efficacy of the privilege claim.

e) Following the receipt of a privilege log, a receiving party may identify, in writing, the particular documents that it believes require further explanation. Within a reasonable time of such an

identification, the producing party must respond to the request.

f) Notwithstanding a claim of privilege, any purportedly privileged document containing non-privileged matter must be: (i) produced with the purportedly privileged portion redacted, with the redacted portion indicated on the document itself, and (ii) listed on the privilege log to be provided above.

g) A privilege log shall be provided by the producing party to the receiving party within ___ days following the delivery of any applicable production, unless there is good cause for delay.

20. In-Camera Review of Documents subject to a Privilege Claim. If a party challenges a request for further information, the parties shall meet and confer to try to reach a mutually agreeable solution. If they cannot agree, the matter shall be brought to the Court. To assist in the prompt resolution of disputed claims of privilege, upon request by the Court, the producing party shall submit to the Court under seal, unredacted copies of all documents for which there is a disputed claim of privilege.

21. Inadvertent Production of Privileged Materials ("Claw-back"). In the event that a producing party claims that it inadvertently failed to designate any production materials or other information as privileged or work-product materials, it shall promptly notify all parties to whom such privileged material was produced or disclosed of the producing party's intent to assert a claim of privilege or work-product over such materials. Upon such notice, the receiving party, if it intends to challenge the designation of the document(s), shall immediately sequester all copies of the document(s), pending Court resolution of the challenge, and shall view and use the document(s) at issue only to the extent necessary to challenge the privilege claim. The document(s) that the receiving party intends to challenge shall only be submitted to the Court under seal for an in-camera review. If the receiving party does not intend to challenge the designation of the document(s), the receiving party shall promptly refrain from further copying or distribution of the subject materials and return or destroy all copies of the subject materials. Where the parties agree, or the Court orders, that an inadvertently produced document is protected by the attorney-client, work-product or other privilege, and such document was originally produced in electronic format on media containing production materials that are not subject to any exemption from production, the producing party shall promptly provide replacement production to the receiving party. The inadvertent production by any producing party, whether in this action or in any other proceedings, of materials subject to a claim of privilege or work-product shall not result in a waiver of any such protection in this action for the produced materials or for any other privileged or immune materials containing the same or similar subject matter. Nor shall the fact of an inadvertent production by any producing party in this action be used as a basis for arguing that a claim of privilege or work-product has been waived in any other proceeding.

22. Receipt of Privileged Information. Nothing in this Protocol shall relieve counsel for any receiving party of any existing duty or obligation, whether established by case law, rule of court, regulation or other source, to return, and not to review, any privileged or work-product materials without being requested by the producing party to do so. Rather, in the event a receiving party becomes aware that it is in possession of what appears to be an inadvertently produced privileged document, then counsel for the receiving party shall immediately: (i) cease any further review of that document; and (ii) notify the producing party of the apparent inadvertent production, requesting whether the producing party intended for the document to be produced. In the event the producing party confirms the inadvertent production of the privileged document, the receiving party shall promptly return or destroy all copies of the inadvertently produced

privileged document in its possession and take reasonable steps to retrieve all copies of the inadvertently produced privileged documents distributed to other counsel or non-parties.

23. e-Discovery Liaison. The parties agree to designate one or more individuals to act as liaisons for purposes of meeting, conferring and attending court hearings regarding discovery of ESI. Regardless of whether the e-Discovery liaison is an attorney (in-house or outside counsel), a third-party consultant or an employee of the party, each e-Discovery liaison must be prepared to accomplish the goals of cooperation set forth above.

.

Appendix A: Metadata Fields to be Included in Load Files

Field Name	Data Example	Field Description
BEGDOC	XYZ 00000178	Bates number of first page.
ENDDOC	XYZ 00000178	Bates number of last page.
BEGATT	XYZ 00000177	Bates number of first page of attachment range. Blank if no attachments.
ENDATT	XYZ 00000179	Bates number of last page of attachment range. Blank if no attachments.
ATTACHMENT	XYZ 00000178; XYZ 00000179	Semicolon separated list of Bates number of first page of each attachment.
PARENTID	XYZ 00000177	It refers to the main email body that the attachments belong to. Bates number of first page of parent. Only populated for attachments.
RECORDTYPE	eEmail	Possible values include Email (Email body), Attachment (Email Attachment), eDoc (Native file).
DATESENT	04/15/2012	Date email was sent in the format MM/DD/YYYY using local time zone provided. If no local time is provided, Universal Time (formerly GMT) is used.
TIMESENT	02:45:22 PM	Time email was sent in the format HH:MM:SS XM using local time zone provided. If no local time is provided, Universal Time (formerly GMT) is used.
DATERECEIVED	04/15/2012	Date email was received in the format MM/DD/YYYY using local time zone provided. If no local time is provided, Universal Time (formerly GMT) is used.
TIMERECEIVED	02:45:22 PM	Time email was received in the format HH:MM:SS XM using local time zone provided. If no local time is provided, Universal Time (formerly GMT) is used.
DATECREATED	04/15/2012	It will show the date that the native file is stored in the properties of the file, when it was first created.
TIMECREATED	02:45:22 PM	Time native file was created in the format HH:MM:SS XM using local time zone provided. If no local time is provided, Universal Time (formerly GMT) is used.
DATEMODIFIED	04/15/2012	Date Last Modified for native files in the format MM/DD/YYYY using local time zone provided. If no local time is provided, Universal Time (formerly GMT) is used.
TIMEMODIFIED	02:45:22 PM	Time native file was modified in the format HH:MM:SS XM using local time zone provided. If no local time is provided, Universal Time (formerly GMT) is used.
LASTMODIFIEDBY	Alex Murphy	The name of the author who was the last person to make changes to the native file(s).

AUTHOR	Jacob Brown	Author for Native files.
FROM	Adam Brooks	Author for Native files. Sender for Emails.
TO	John Doe (jdoe@domain.com);	Semicolon separated list of Recipients for Email. The exact value depends on multiple factors including the email client address book. This includes name, email address, and/or Moniker.
CC	John Junior (jjunior@domain.com);	Semicolon separated list of Carbon Copy Recipients for Email. The exact value depends on multiple factors including the email client address book. This includes name, email address, and/or Moniker.
BCC	Sarah Smith (ssmith@domain.com)	Semicolon separated list of Blank Carbon Copy Recipients for Email. The exact value depends on multiple factors including the email client address book. This includes name, email address, and/or Moniker.
SUBJECT	Meeting time changed	Subject of the email.
FILENAME	Proposed Retainer - clean copy	Filename without extension of the native file.
FILEEXTENSION	.doc	File extension of native file.
VOLUME	PROD_IMG001	Fixed.
ORIGINALSPATH	\ORIGINALS\001\XYZ 00000177.xlsx	Relative file path of Native files.
PAGES	20	Number of pages if file was converted to PDF or TIFF.
SOURCEFILEPATH	ORIGINALS\001\XYZ 00000177.xlsx	Relative file path of Native files. It refers to the Folder Path within Microsoft Outlook and keeping folders and subfolders information.
TEXTPATH	\TEXT\001\XYZ 00000177.TXT	Relative file path of Extracted / OCR text.
PDFPATH	\PDF\0001\TEST 0000001.pdf	Relative file path of PDF files.
CUSTODIAN	Malta	Custodian associated with Original (native) file.
MD5	C8054025235FBRA26E4BC242A EF543B6	Incoming MD5 of Original (native) file.