UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

IN RE: CHANGE HEALTHCARE, INC. CUSTOMER DATA SECURITY BREACH LITIGATION

Case No. 24-md-3108 (DWF/DJF)

ESI ORDER

This Order Applies to All Actions

This matter is before the Court on the parties'[1] Joint Statement Regarding the Proposed Electronically Stored Information Protocol, Protective Order, Coordination Order, and Discovery ("Joint Statement") (ECF No. 234). Based on the parties' Joint Statement and for good cause shown, the procedures and protocols outlined herein ("ESI Protocol") shall govern the production of electronically stored information ("ESI") and paper ("hardcopy") documents by the parties in the above-captioned action (the "Action"). Unless otherwise agreed to by the Parties, nothing in this ESI Protocol shall limit a Party's right to seek or object to discovery as set out in applicable rules or to object to the authenticity or admissibility of any hardcopy document or ESI produced in accordance with this ESI Protocol.

The Parties acknowledge the intent of the ESI Protocol is to facilitate efficient and proportional discovery of ESI and to promote, to the fullest extent possible, the resolution of disputes regarding the discovery of ESI without Court intervention.

I. DEFINITIONS

a. "Parties" collectively shall mean all named Parties to this Action, including any Party added or joined to any complaint in this Action, as well as named Parties to actions that may

[1] Plaintiffs and Defendants include all those named in the Consolidated Complaints filed on January 15, 2025.

be consolidated into or coordinated with the above-captioned Action.

b. "Producing Party" means any Party or third-Party to this Action who produces documents or ESI pursuant to any discovery request, subpoena, or otherwise.

c. "Receiving Party" means a Party or third-Party to this Action who receives documents or ESI from a Producing Party in response to a discovery request, subpoena, or otherwise.

II. GENERAL PROVISIONS

a. **General.** The purpose of this ESI Protocol is to facilitate the exchange of ESI (as defined in Fed. R. Civ. P. 34(a)(1)(A)) and hard copy documents in an efficient manner and in accordance with the Federal Rules.

b. **Applicability.** This ESI Protocol governs the production of documents and information in this Action. Nothing in this ESI Protocol is intended to be an exhaustive list of discovery obligations or rights of the Parties under the Federal Rules of Civil Procedure or the Local Rules of the United States District Court for the District of Minnesota ("Minnesota Local Rules") or any other applicable statutes, orders, and rules. To the extent additional obligations or rights not addressed in this ESI Protocol arise under the Federal Rules of Civil Procedure or the Minnesota Local Rules, or any other applicable statutes, orders, and rules, they shall be controlling.

c. **Limitations and Non-Waiver.** The Parties and their attorneys do not intend by this ESI Protocol to waive their rights to any protection or privilege, including but not limited to, the attorney-client privilege, the work-product doctrine, and any other privilege or immunity that may be applicable. The Parties and their attorneys are not waiving, and specifically reserve, the right to object to any discovery request on any grounds. This ESI Protocol does not govern the appropriate scope of discovery under Rule 26(b)(1), custodian selection and search parameters, or

impose any obligations beyond the Federal Rules of Civil Procedure or the Minnesota Local Rules.

d. **Authenticity, Relevance, Discoverability, and Admissibility.** Nothing in this ESI Protocol shall be construed to affect the authenticity, relevance, discoverability, or admissibility of any document or data. All objections to the authenticity, relevance, discoverability, or admissibility of any document or data are preserved and may be asserted at any time.

e. **Modification by Agreement.** Any practice or procedure set forth herein may be modified by written agreement of the Parties. Any Party added or joined to this Action and any Party to actions that may be consolidated into or coordinated with this Action after the date of this ESI Protocol that seeks to deviate from the ESI Protocol set forth herein must obtain leave of Court to do so unless all Parties otherwise consent in writing.

f. **Modification by Court Order.** Nothing in this ESI Protocol waives the right of any Party to petition the Court for an Order modifying its terms upon good cause shown, provided, however, that counsel for such Party must first meet and confer with counsel for the opposing Party, and the Parties shall use reasonable efforts to negotiate an amendment of this ESI Protocol prior to seeking relief from the Court.

g. **Variations**: If any Party identifies a specific circumstance where application of this Order is not technologically practicable, the Party will disclose to all other Parties the reason(s) for, and circumstances surrounding, the need to vary from this Order in that particular circumstance, and the Parties will meet and confer in an effort to reach agreement on an appropriate deviation from this Order. In the event the Parties cannot reach agreement, the matter may be submitted to the Court for determination.

h. **Prior Productions**. Responsive documents and ESI previously collected and

produced outside of this Action will be re-produced in this Action in the same form and manner that they were previously produced, even if such re-production is not in conformance with the provisions of this Order. Following receipt of such documents, the Receiving Party may request the documents be produced in conformance with the provisions of this Order. In the event the Parties cannot reach agreement, the matter may be submitted to the Court for determination.

i. **Protective Order**. Nothing herein shall contradict the Parties' rights and obligations under the Protective Order and Qualified HIPAA Protective Order ("Protective Order"). If there is any inconsistency between this ESI Protocol and the Protective Order, the terms of the Protective Order shall govern.

III. PRESERVATION

The Parties agree that they shall continue to take reasonable efforts to preserve potentially relevant documents and ESI, including Metadata identified in **Appendix A**, in accordance with their obligations under the Federal Rules of Civil Procedure and other applicable law. The Parties agree that by preserving documents or providing information about the Parties' preservation efforts the Parties are not conceding that such material is discoverable.

IV. PRODUCTION OF STRUCTURED DATA

To the extent a response to discovery implicates ESI contained in a structured database, the Parties shall meet and confer regarding the exchange of available information concerning such databases. Such information may include, to the extent available, data fields/objects, data dictionaries and schema, the nature of the data contained in structured data sources, the types of information stored in the database(s), the types of reports that can be or were generated from or for the data and how and whether specialized queries may be run, whether there are existing and reasonably available reports that include the information, if the nature of the data stored in a field

is not clear from the name of the field, and whether the Receiving Party will need any additional information. To the extent information is not available in its native form, the Parties agree to meet and confer regarding what format would be reasonably available.

V. IDENTIFICATION OF RESPONSIVE DOCUMENTS

a. The Parties agree that each Producing Party will take reasonable efforts to identify, review, and produce relevant ESI.

b. While this ESI Protocol is intended to address the majority of documents and data sources handled in this matter, there may be situations where the Parties come into contact with data sources that are not specifically addressed herein. In the event such data sources contain responsive information and are relevant, the Parties agree to take reasonable efforts to address such data sources appropriately, and, upon request of the Receiving Party, to meet and confer regarding search parameters and relevant production formats for such ESI. The parties shall identify the location, platform, and sources of any relevant ESI.

c. The Parties shall cooperate in the development of appropriate search methodology and criteria, including the potential use of Technology Assisted Review ("TAR") and/or potential use of AI. By agreeing to use TAR and/or AI in this action, the Producing Party does not intend to waive any rights or protections pursuant to privacy, confidentiality, attorney-client privilege, attorney work product, and any other privileges, protections, or objections to discovery.

d. The Parties will meet and confer and attempt in good faith to reach agreement regarding the following: (i) the identity of custodians (and non-custodians) who may have discoverable ESI; (ii) the number of custodians from whom ESI should be searched; (iii) the search terms, phrases, or parameters to be used in searching databases for responsive ESI; (iv) the applicable timeframe for collection and review of documents; and (v) if TAR and/or AI is to be

used, the parameters of the TAR and/or AI model, including the criteria for evaluating and accepting the results of the TAR and/or AI model. A producing party may use any methodology and tool for the purpose of prioritization and/or expediting the review, so long as no documents are removed from attorney review or production based on such methodology. The parties will produce known responsive documents regardless of whether the search terms, TAR and/or AI process identifies such known responsive documents.

e. Non-Discoverable Information. The Parties agree that the following data categories shall be deemed inaccessible and therefore, not discoverable, and should not be preserved:

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

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

iii. Online access data such as temporary internet files, history, cache, cookies, and the like.

iv. Data in metadata fields that are frequently updated automatically, such as last opened date.

v. Backup and archive data that are substantially duplicative of data that are more accessible elsewhere.

vi. Data remaining from systems no longer in use that is unintelligible on the systems in use and where there is no reasonable way to convert the data to a universal format such as CSV, XLSX, TXT, SQL, XML, etc.

vii. Data from personal information management applications (such as Microsoft Outlook) (e.g., email, calendars, contact data, and notes) sent to or from mobile devices (e.g., iPhone, iPad, or Android, and 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).

f. Quarantined Data. If data is requested from servers that a Party has quarantined for the security of its systems and/or network, the Parties shall meet and confer and consult with information technology consultants or employees to determine whether there is a reasonable way to retrieve the data without compromising the security of the Producing Party's systems and/or network. If no reasonable way to retrieve the data without compromising security exists, the data shall be deemed inaccessible, and therefore, not discoverable. If, after meeting and conferring in good faith, the parties dispute whether retrieval of the data is reasonable, the Parties may seek a determination from the Court.

g. Inaccessible Documents. If a Party responding to a discovery request believes any potentially relevant documents are not reasonably accessible, that Party will provide sufficient information, including the underlying basis for why such documents are not reasonably accessible (to the extent such information is not privileged), about the documents (and their custodial or non-custodial sources) to enable the Parties to meet and confer in good faith about whether such documents will be produced.

VI. PRODUCTION OF DOCUMENTS ORIGINATING AS PAPER

The following production specifications apply to documents that existed in paper format prior to production ("Hard Copy Documents"). Documents that originated as paper but which were scanned and maintained electronically by a Party prior to the filing of any Consolidated Complaint in this Action shall be produced in accordance with Part VII of this ESI Protocol. The Parties agree to produce Hard Copy Documents in the formats described below, to the extent reasonably practicable and not unduly burdensome. These formats are deemed to be productions

in reasonably usable form. If a Producing Party intends to produce any Hard Copy Documents in any manner other than as specified herein, the Producing Party shall notify the Receiving Party of its intent, including production format (e.g., produced as paper, made available for inspection). If the proposed production format is not acceptable to the Receiving Party, the Parties shall meet and confer to determine a mutually acceptable production format for such Hard Copy Documents.

a. **TIFFs.** Hard Copy Documents should be scanned as single-page, black and white, Group IV compression TIFF images using a print setting of least 300 dots per inch (DPI). Bates numbers, confidentiality designations (in accordance with the Protective Order), and redactions (to the extent they are necessary) should be burned into the image. TIFF image files should be provided in an "Images" folder.

b. **Unitizing Documents.** The Parties shall undertake reasonable efforts to ensure that, in scanning paper documents, distinct documents should not be merged into a single record, and single documents should not be split into multiple records (i.e., paper documents should be logically unitized). For example, the Parties shall undertake reasonable efforts to produce documents stored in a binder, folder, or similar container (each a "container") in the same order as they appear in the container. The front cover of the container should be produced immediately before the first document in the container. The back cover of the container should be produced immediately after the last document in the container. The relationship among the documents in the container should be reflected in the proper coding of the beginning and ending document and attachment fields.

c. **OCR.** Hard Copy Documents shall be run through optical character recognition ("OCR") software, and the full text shall be provided on a document-level in an appropriately formatted text file (.txt) that is named to match the first Bates number of the document. Text files

should be provided in a "Text" folder. To the extent that a document is redacted, the text files should not contain the text of the redacted portions.

d. **Unique IDs.** Each TIFF image should have a unique filename, which corresponds to the Bates number of that page. The filename should not contain any blank spaces and should be zero-padded (e.g., ABC-000001), taking into consideration the estimated number of pages to be produced. If a Bates number or set of Bates numbers is skipped in a production, the Producing Party will so note in a cover letter or production log accompanying the production or as soon as practicable thereafter. Bates numbers will be unique across the entire production and prefixes will be consistent across all documents a Party produces in the Action.

e. **Data Load Files.** Hard Copy Documents should be provided with an Opticon Cross-Reference File and Concordance data load file using standard Concordance delimiters:

i. Field Separator: ASCII character 20 ("¶");

ii. Quote: ASCII character 254 ("þ"); and

iii. New Line: ASCII character 174 ("®").

iv. Concordance-compatible image and data load files should be provided in a "Data" folder.

f. **Metadata.** Each of the Metadata and coding fields set forth in **Appendix A** shall be produced for that Hard Copy Document to the extent reasonably available. For documents that are partially redacted for privilege, the parties are not required to produce corresponding privileged metadata fields.

g. **Color.** Hard Copy Documents containing color need not be produced in color in the first instance, provided however, that the Producing Party shall retain a copy of produced hard copy documents in color. The Receiving Party may request production of such documents in color

by providing a list of the Bates numbers of documents it requests to be produced in color format.

VII. PRODUCTION FORMAT FOR ELECTRONICALLY STORED INFORMATION

The Parties agree to produce ESI in the formats described below. These formats are deemed to be productions in reasonably usable form. If any Party contends that particular documents or ESI warrant a different format, the Parties will meet and confer to determine a mutually acceptable production format for such documents.

a. **TIFFs.** Documents should be produced as single-page, black and white, Group IV TIFF images using at least 300 DPI. To the extent possible through an automated process, the document's original orientation should be maintained (i.e., portrait-to-portrait and landscape-to-landscape). In the event the original orientation of documents in a production appears to be altered (e.g., emails are inverted or sideways) the Receiving Party may request the reproduction of those documents in their original orientation. Bates numbers, confidentiality designations (in accordance with the Protective Order), and redactions (to the extent they are necessary) should be burned into the image. TIFF image files should be provided in an "Images" folder.

b. **Extracted Text Files.** The full text of native files should be extracted directly from the native file and should be delivered in an appropriately formatted text file (.txt) that is named to match the first Bates number of the document. Text files should be provided in a "Text" folder. To the extent that a document is redacted, the document should undergo OCR after the text has been redacted in order to remove the redacted text.

c. **Unique IDs.** Each image should have a unique filename, which corresponds to the Bates number of that page. The filename should not contain any blank spaces and should be zero-padded (e.g., ABC-000001), taking into consideration the estimated number of pages to be produced. If a Bates number or set of Bates numbers is skipped in a production, the Producing

Party will so note in a cover letter or production log accompanying the production or as soon thereafter as practicable. Bates numbers will be unique across the entire production and prefixes will be consistent across all documents a Party produces in this Action.

d. **Parent-Child Relationships.** The Parties agree that if any part of an email or its attachments is responsive, the entire email and attachments must be produced, except any attachments that must be withheld or redacted on the basis of privilege, work-product, or other protection. The Parties shall take reasonable efforts to ensure that parent-child relationships within a document family (the association between an attachment and its parent document) are preserved, including any attachments to emails subsumed within an email thread. The child-document(s) should be consecutively produced immediately after the parent-document. Each document shall be produced with the production number for the first and last page of that document in the "BegBates" and "EndBates" fields of the data load file and with the "BegAttach" and "EndAttach" fields listing the production number for the first and last page in the document family.

e. **Hyperlinks**. If a production includes hyperlinks to documents that a Party believes may be responsive and the hyperlinked documents are not otherwise produced, the Party may request that the hyperlinked documents be produced. If, after meeting and conferring in good faith, the Parties dispute whether retrieval of the hyperlinked documents is reasonable, the Parties may seek a determination from the Court.

f. **Metadata.** The Parties agree that Metadata will be produced for all produced documents and ESI, whether produced in Native Format or as TIFF images, to the extent that such information is reasonably available. **Appendix A** sets forth the metadata fields that must be produced to the extent that metadata exists for a particular document. For documents that are partially redacted for privilege, the parties are not required to produce corresponding privileged

metadata fields. Nothing herein shall require any Party to create or produce metadata that does not exist or is not reasonably or technically accessible.

g. **Native Format.** The processed native for all spreadsheets (i.e., MS Excel, .CSV, or similar), PowerPoints, and electronic information containing audio or video components should be produced and linked to the database by the metadata field "NativeLink." Where native files are produced in lieu of TIFF images, each native file will be assigned a unique Bates number. The Producing Party will produce a placeholder (a single-page TIFF slip sheet indicating that the native item was produced) along with the file itself in Native Format. The placeholder will be branded with the production number in the lower right hand corner and the phrase "PRODUCED IN NATIVE ONLY" branded in the center of the page. The Producing Party will also brand any confidentiality or similar endorsements in the lower left hand corner of the placeholder.

h. **Redaction of Native Files.** Spreadsheets shall be redacted in native format using eDiscovery industry best practices. The natively redacted file shall be produced as a native file.

i. **Request for Native Files.** Other than as specifically set forth above, a Producing Party need not produce documents in Native Format. If good cause exists for the Receiving Party to request production of certain documents in Native Format, the Receiving Party may request production in Native Format by providing a list of the Bates numbers of documents it requests to be produced in Native Format. The Producing Party shall not unreasonably deny such requests. Producing Party shall produce an overlay to ensure that the "NativeLink" entry in the data load file indicates the relative file path to each Native File in such production, and all Extracted Text and applicable metadata fields.

j. **Hidden Content.** To the extent that a document or ESI was saved with hidden content, such as comments or tracked changes, the document or ESI shall be imaged showing that

hidden content, to the extent the Producing Party can practicably do so using an automated process. If for any reason a document containing hidden content is identified via an automated process but cannot be imaged to show all hidden text, it will be produced in Native Format.

k. **Password Protected Files.** The Parties agree that they will take reasonable efforts to unencrypt and index any password-protected documents or other encrypted containers prior to applying search terms, TAR, AI, or other filtering methodologies. To the extent security protection for such documents and ESI cannot be successfully processed despite reasonable efforts, the Producing Party shall notify the Receiving Party of the number of documents affected for each custodian and agree to meet and confer should the Receiving Party request additional information about such files.

l. **Embedded Documents.** Non-image files embedded within documents, such as spreadsheets within a PowerPoint, will be extracted as separate documents and treated like attachments to the document in which they were embedded. The Bates number of the source file from which the embedded file is extracted shall be provided as metadata associated with the embedded file, as described in **Appendix A**. Graphic objects embedded within documents or emails, such as logos, signature blocks, and backgrounds need not be extracted as separate documents.

m. **Data Load Files**. Documents should be provided with an Opticon Cross-Reference File and Concordance data load file using standard Concordance delimiters:

i. Text Delimiter AKA "Quote" – "þ", Hex (FE), Unicode (U+00FE), Decimal (254) 2;

ii. Field Separator AKA "Comma" – "", Hex (14), ASCII character 20 ("¶");

iii. Unicode (U+0014), Decimal (20);

iv. Quote: ASCII character 254 (“þ”); and

v. New Line: ASCII character 174 (“®”).

All rows will contain the same number of delimiters and fields. The multi-value field delimiter must be consistent across all fields. Concordance-compatible image and data load files should be provided in a “Data” folder. Parties have the option to exchange sample load files. If this exchange occurs, the Receiving Party will have 14 days to respond with Load File change requests. Nothing in this ESI Protocol will limit the Parties from discussing Load File changes throughout the course of the Action.

n. **Deduplication.** A Producing Party may globally deduplicate by exact duplicate families provided that: (i) only exact hash duplicates are subject to deduplication; (ii) the Producing Party identifies the additional custodians in an CustodianAll metadata field; (iii) the Producing Party identifies the additional file paths in an AllPaths metadata field; and (iv) an email that includes content in the BCC or other blind copy fields shall not be treated as a duplicate of an Email that does not include content in the BCC or other blind copy field, even if all remaining content in the email is identical. Standalone files may be de-duplicated against other stand-alone files, but not against attachments contained in document families.

o. **Email Threading.** Email threads are email communications that contain prior or lesser-included email communications that also may exist separately in the Party’s electronic document collection. The Parties reserve the right to use email threading to facilitate production of the most inclusive email, reduce the overall amount of ESI and documents produced, and use email thread suppression to avoid review and production of information contained within an existing email thread in another document being reviewed and produced. A most inclusive email thread is one that contains all of the prior or lesser-included emails, including attachments, for that

branch of the email thread. For the avoidance of doubt, only email messages for which the parent document and all attachments are contained in the more inclusive email message will be considered less inclusive email messages that need not be produced; if the later message contains different text (such as where the later message adds in-line comments to the body of the earlier message), or does not include an attachment that was part of the earlier message, the earlier message must be produced.

p. **Production of Audio and Video Recordings.** The Parties shall meet and confer before producing audio and video recordings other than in their native format.

q. **Production of Transcripts.** If deposition or other transcripts are responsive, the Parties should meet and confer to determine a mutually agreeable format for producing the transcripts.

r. **Custodian or Originating Source.** The Custodian shall be identified in the Custodian field of the database load files. Documents collected from a natural person should be produced in such fashion as to identify the natural person. Documents collected from non-custodial sources, such as shared files, storage locations, or drives, should be produced in such a fashion as to identify them as non-custodial sources (e.g., CORP.). A Producing Party shall make reasonable efforts to use a uniform description of a particular Custodian across productions.

s. **Color.** Documents containing color need not be produced in color in the first instance, provided however, that the Producing Party shall retain a copy of produced documents in color. The Receiving Party may request production of such documents in color by providing a list of the Bates numbers of documents it requests to be produced in color format.

t. **Foreign Language.** Foreign language text files and Metadata should be delivered with the correct encoding to enable the preservation of the document's original language.

u. **Date Format.**

i. If a time is not available, such as the estimate date for a coded document, then 12:00 am, or 00:00 should be assigned, i.e., 12/21/1999 00:00.

ii. Date delimiters, such as slashes and colons, must be consistent across all fields. In the format of MM/DD/YYYY, there are no spaces and only forward slashes.

iii. Date formats must be consistent within any one field.

iv. Date formats must be consistent across all fields, i.e., a record with a sent date should have the same format in the last modified date field.

v. Unless otherwise specified by a Producing Party, the Producing Parties shall process all ESI using CST as the time zone.

v. **Production Media.** The preferred means of producing documents is via secure FTP or secure file share. However, documents may also be produced via encrypted flash drive, encrypted hard drive. Physical media should be encrypted before it is produced.

w. **Naming Convention for Production Media.** Whether produced via secure FTP, file share, or physical media, the files produced should be combined into a compressed file such as .zip, .rar, etc. The compressed file should be named so as to indicate Producing Party, and the sequence of the production (e.g., "CHC-001"). If the production is made using physical media, the media should be labeled to include: (a) text referencing that it was produced in *In re: Change Healthcare, Inc. Data Breach Litigation*; and (b) the Bates number range of the materials contained on the media. With every production, the Producing Party shall include a cover letter that includes the date(s) of the production.

x. **Replacement Productions.** Any replacement production will be transmitted with

a cover letter or email to identify the production as a replacement and cross-reference the BegBates and EndBates of the documents being replaced. If the replacement production is being transmitted by physical media, the media shall include the phrase "Replacement Production."

y. **Encrypted Data.** To the extent a production is encrypted before it is produced, the Producing Party shall contemporaneously transmit the credentials necessary to decrypt the data.

z. **Confidentiality Designations.** If a particular paper document or ESI item qualifies for confidential treatment pursuant to any applicable federal, state, or common law (e.g., Personally Identifiable Information or Protected Health Information), or pursuant to the terms of the Protective Order, the designation shall be branded on the document's image at a location that does not obliterate or obscure any part of the underlying images. This designation also should be included in the appropriate data field in the load file. For documents produced in native format with image placeholders, the placeholder image for the native file should be branded with the appropriate confidentiality designation to the extent possible. Receiving Parties shall ensure that the confidentiality claim follows the document regardless of whether the designation imprints on the file when viewed in printed form. A Party's failure to comply with the procedures set forth in this ESI Protocol shall not waive that Party's or any other person's right to assert that information is private, confidential, or otherwise protected.

VIII. ASSERTIONS OF PRIVILEGE

To the extent any Party withholds documents based on privilege that fall under this ESI Protocol, that Party must comply with the terms set forth in the Protective Order.

IX. THIRD PARTY DOCUMENTS

This Order shall govern productions made by any non-Party who is subpoenaed in this action unless otherwise agreed to by the Parties. A Party that issues a non-Party subpoena

("Issuing Party") shall include a copy of this ESI Protocol with the subpoena and state that the Parties to the Action have requested that third-Parties produce documents in accordance with the specifications set forth herein. The Issuing Party shall promptly notify the other Parties when it receives non-Party productions, and shall provide copies of such productions to the other Parties in the format in which they were received from the third-Party within seven business days. In the event that the format of a third-Party production does not conform with the specifications set forth herein, the Parties shall meet and confer regarding the format of production to Receiving Parties. Nothing in this ESI Protocol is intended to or should be interpreted as narrowing, expanding, or otherwise affecting the rights of the Parties or third Parties to object to a subpoena.

IT IS SO ORDERED.

Dated: March 18, 2025

s/ Dulce J. Foster
Dulce J. Foster
United States Magistrate Judge

APPENDIX A: REQUIRED METADATA FIELDS

Field Name[2]	Populated For	Field Description
BegBates	All	Control Numbers for start of document
EndBates	All	Control Numbers for end of document
BegAttach	All	Control Numbers (First production Bates number of the first document of the family)
EndAttach	All	Control Numbers (Last production Bates number of the last document of the family)
Attachment Count	All	Number of attachments
Custodian	All	Custodian name (ex. John Doe)
CustodianAll	All	All custodians who were in possession of a de-duplicated document besides the individual identified in the Custodian field
LogicalPath	All	The directory structure of the original file(s) at the time of collection. Any container name is included in the path. For email, this should include the email folder path from which the email was collected.
AllPaths	All	This field should be populated with the folder paths of all duplicate files (Email and Edocs) that were suppressed during deduplication.
Hash value	All	The MD5 or SHA-I hash value
PgCount	All	Page Count or an Image Count, if auto generated
EmailSubject	Email	Subject line of email
DateSent (mm/dd/yyyy hh:mm)	Email	Date email was sent
TimeZoneUsed	Email	Time zone used to process data during document collection and processing
ReceiveDate (mm/dd/yyyy hh:mm)	Email	Date email was received
To	Email	All recipients that were included on the "To" line of the email
From	Email	The name and email address of the sender of the email

[2] The Field Names and Descriptions in this ESI Protocol are meant to serve as a guide; the Parties acknowledge that Field Names can vary from system to system and even between different versions of systems.

CC	Email	All recipients that were included on the "CC" line of the email
BCC	Email	All recipients that were included on the "BCC" line of the email
DateCreated (mm/dd/yyyy hh:mm)	Edoc	Date the document was created
FileName	Email, Edoc	File name of the edoc or email
Title	Edoc	Any value populated in the Title field of the document properties
Subject	Edoc	Any value populated in the Subject field of the document properties
Author	Edoc	Any value populated in the Author field of the document properties
DateMod (mm/dd/yyyy hh:mm)	Edoc	Date the document was last modified
LastModifiedBy	Edoc	Last person who modified (saved) a document
DocExt	All	File extension of the document
Redacted	All	"X," "Y," "Yes," and "True" are all acceptable indicators that the document is redacted. Otherwise, blank
Confidentiality	All	Populated if document has been designated as "Confidential" or "Highly Confidential" under the Protective Order
Production Volume	All	Production Volume Name
DocType	All	Description of document (Email, Attachment, EDoc, Hard Copy, etc.)
Email Thread ID	Email	Unique identification number that permits threading of email conversations. For instance, unique MS Outlook identification number ("PR_CONVERSATION_INDEX") is 22 bytes in length, followed by zero or more child blocks each 5 bytes in length, that facilitates use of email threading.
Importance	Email	Notation created for email messages to note a higher level of importance than other email messages added by the email originator
FileSize	All	Size of native file, in bytes.
SuspectOLE	Edoc	The yes/no indicator of whether a file such as a Microsoft Word document has additional files embedded in it.

Comments	Edoc	Comments extracted from the metadata of the native file
HasTrackChanges	Edoc	The yes/no indicator of whether the track changes metadata on an Office document is set to True.
HiddenText	Edoc	Indication of the existence of hidden document data such as hidden text in a Word document, hidden columns, rows, or worksheets in Excel, or slide notes in PowerPoint.
TextPath	All	Relative path to the document level text file
NativeFile	All	Native File Link for documents provided in native format only