UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

IN RE: AT&T, INC. CUSTOMER DATA SECURITY BREACH LITIGATION	Case No. 3:24-cv-00757-E
	MDL DOCKET NO. 3:24-md-03114-E
This Document Relates To All Cases	

CASE MANAGEMENT ORDER # 14

STIPULATED PROTOCOL AND ORDER FOR DISCOVERY OF DOCUMENTS AND ELECTRONICALLY STORED INFORMATION

Pursuant to the negotiated agreement between counsel for Plaintiffs and counsel for Defendants set forth herein, this Court approves, adopts, and orders entry of the following Protocol regarding the standards and procedures for the preservation, collection, review and production of Hard Copy Documents, Electronic Documents or Data, and Electronically Stored Information or ESI (collectively, "Documents") in this complex, multi-district litigation ("Litigation"). This Order applies to all cases now pending in MDL 3114, as well as to any cases later filed in, transferred to, or removed to this Court and included as part of MDL 3114.

This Order is designed to implement and promote an efficient and effective discovery process so that Documents are preserved, identified, collected, reviewed, and produced in a timely fashion by the Named Class Representatives and Defendant(s), avoiding unnecessary, costly, or time-consuming discovery disputes, protecting applicable privileges, and positioning the Parties and the Court to move this MDL to resolution by motion, trial, or settlement.

Nothing in this Order is intended to alter or affect the scope of applicability of the Federal Rules of Civil Procedure, the Local Rules of the U.S. District Court for the Northern District of Texas, or the Court's Standing Orders for Civil Cases, and this Order does not affect the right of any Party to object to a discovery request or to operate as a waiver of any Party's right to

promulgate, object to, or seek relief from a discovery request. Nor does anything in this Protocol create or impose additional obligations or burdens beyond those required by the above-referenced rules. The Parties expressly reserve all objections under the Federal Rules of Civil Procedure and applicable decisional authority relating to the production of Documents.

The Parties acknowledge their duty to work together cooperatively throughout the discovery process. The Parties shall cooperate in good faith and be reasonably transparent in all aspects of the discovery process, including the preservation, identification, collection, review, and production of potentially relevant Documents. Consistent with the Court's Appointment Orders (Dkts. 198 and 199), the Parties shall cooperate and work with the Special Masters to avoid, address, and resolve discovery disputes in a timely and efficient manner.

I. DEFINITIONS

1. "And" and "or" shall be construed conjunctively or disjunctively as necessary to make their use inclusive rather than exclusive, *e.g.*, "and" shall be construed to mean "and/or."

2. "Cloud" shall be broadly interpreted to mean any Web-based software, storage, hosting, messaging, or collaboration service used by Defendant(s) or Defendant(s)' employees, agents, consultants, or vendors.

3. "Custodial Data" is data that is created, sent, received, stored or managed by an Individual Custodian.

4. "Document(s)" is defined to be synonymous in meaning and equal in scope to the usage of this term in Rules 26 and 34 of the Federal Rules of Civil Procedure. The term "Document" shall include Hard Copy Documents, Electronic Documents or Data, and Electronically Stored Information as defined herein.

5. "Electronic Document(s) or Data" means electronic documents or files existing in electronic form at the time of creation or collection, including but not limited to e-mail, text

messages, chats, posts, or any other forms or means of electronic communications, word processing files (*e.g.*, Microsoft Word), computer presentations (*e.g.*, PowerPoint slides), spreadsheets (*e.g.*, Excel), image files (*e.g.*, .jpg and .pdf), and video and audio files.

6. "Electronically Stored Information" or "ESI," as used herein has the same meaning as defined in Federal Rule of Civil Procedure 26 and 34, and includes, Electronic Documents or Data, and computer-generated information or data, created or stored in or on any storage media located on computers, servers, mobile or handheld devices, tablets, "Cloud" repositories or depositories, disks, USB or thumb drives, external hard drives, tapes, or other real or virtualized devices or digital media.

7. "Hard Copy Document(s)" means Documents existing in physical tangible form at the time of creation or collection, including but not limited to paper Documents.

8. "Hash Value" is a numerical identifier that can be determined from a file, a group of files, or a portion of a file, based on a standard mathematical algorithm that calculates a value for a given set of data, serving as a digital fingerprint, and representing the binary content of the data to assist in subsequently ensuring that data has not been modified and to facilitate duplicate identification. Unless otherwise specified, hash values shall be calculated using the MD5 hash algorithm.

9. "Individual Custodian(s)" are natural persons whose communications, files, and electronically stored information may be relevant to the claims or defenses in the Litigation. Such data may include email accounts, local device storage (e.g., laptops or desktops), and individual cloud accounts (e.g., Google Drive or OneDrive).

10. "Load File(s)" means electronic files provided with a production set of Electronic Documents or Data or ESI and images and used to load that production set into the document review platform of the Party receiving a production and for the correlation of such data within that

platform by conveying information identifying a set of document images, processed ESI, or Native Format files, as well as the corresponding extracted full text or OCR text files, and containing agreed-upon extracted or user-created metadata as well as information indicating physical and logical unitization (*i.e.*, document breaks and document relationships such as those between an e-mail and its attachments). A load file is used to import all image, native, and text files and their corresponding production information into a review database. The Party producing Documents shall produce a Load File for all produced Documents with each particular production in accordance with specifications provided herein.

11. "Metadata" means: (i) information embedded in a Native Format file that is not ordinarily viewable or printable from the application that generated, edited, or modified such Native file, and (ii) information generated automatically by the operation of a computer or other information technology system when a Native file is created, modified, transmitted, deleted, or otherwise manipulated by a user of such system, and for purposes of this Protocol (iii) information, such as Bates numbers and Hash Values, redaction status, privilege status, or confidentiality status created during the course of processing Documents or ESI for production.

12. "Native Format" or "Native" means the file format associated with the application by which it was originally created as collected from Individual Custodians or Non-Custodial sources. For example, the native format of an Excel workbook is an .xls or .xlsx file.

13. "Non-Custodial Data" is data that is stored or managed by System or Database Custodians. "Optical Character Recognition" or "OCR" means a technology process that captures text from an image for the purpose of creating an ancillary text file that can be associated with the image and searched in a database. OCR software evaluates scanned data for shapes it recognizes as letters or numerals.

14. "Party" or "Parties" means the Named Class Representatives listed in the

Consolidated Amended Complaint and/or Defendant AT&T, Inc. and any other Defendants named, joined, or impleaded in this matter.

15. "Producing Party" means the Party producing Documents in response to any Request for Production of Documents pursuant to Fed. R. Civ. P. 34(a) or any other discovery request.

16. "Receiving Party" means the Party receiving Documents pursuant to Fed. R. Civ. P. 34(a) or any other discovery request.

17. "Requesting Party" means the Party requesting Documents pursuant to Fed. R. Civ. P. 34(a), or for any other discovery request.

18. "Searchable Text" means the native text extracted from Electronic Documents or Data or ESI or, when extraction is infeasible, by Optical Character Recognition text ("OCR text") generated from a Hard Copy Document or electronic image.

19. "System or Database Custodian(s)" are persons or entities responsible for the maintenance, operation, or oversight of enterprise systems, databases, or shared repositories. These custodians may not be the creators of the data but have administrative control or access to centralized datasets holding information that may be relevant to the claims or defenses in the Litigation.

20. "Unitization" means the assembly of a set of scanned Hard Copy Documents and indicates where individual pages or files belong together as Documents for functional, archival and retrieval purposes. Unitization includes both (i) Logical Unitization, being the determination of pages that belong together as Documents and which capture family relationships such as a parent Document or message and its attachments, and (ii) Physical Unitization, which captures the assembly of individually scanned pages into Documents and where each Document begins and ends. Physical Unitization normally uses objects such as staples, paper clips, and folders to

determine pages that belong together as Documents for functional, archival, and retrieval purposes.

II. PRESERVATION

1. The Parties represent that they have or will issue preservation or litigation hold notices to those Individual Custodians likely to have potentially relevant Documents. The Parties understand their ongoing obligation to identify systems or databases that contain potentially relevant Documents and issue preservation or litigation hold notices to appropriate System or Database Custodians and suspend any destruction and/or purging policies pertaining to such systems. The Parties represent that they have established procedures to ensure that those preservations notices have been received. The Parties will preserve any preservation or litigation hold notices and the dates of receipt. Where a custodian has not received a hold notice directly, the Parties will preserve the date that the Party implemented a litigation hold for such Custodian. The Parties further represent that they are preserving potentially relevant Non-Custodial Data, including Metadata identified in Appendix A where it exists, in accordance with their obligations under common law. The Parties will meet and confer regarding the scope of preservation, including Custodial and Non-Custodial Data, date ranges, and categories of information that have been or should be preserved in connection with this Litigation in accordance with this Order. 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. Specifically, the Parties agree to:

i. Preserve potentially relevant e-mail, messages, chats, or posts on any enterprise or third-party communication or collaboration tools, software, or platforms, whether or not authorized for business, if deemed to contain potentially relevant information by the Producing Party and to the extent that the Producing Party has possession, custody or control over such information, such as, and by way of example only Microsoft Teams, Zoom, Google Chat, Slack,

Telegraph, Signal, WeChat, etc.; and

ii. Suspend processes and procedures which would result in the loss or transfer to a less-accessible medium of any potentially relevant Documents.

III. E-DISCOVERY LIAISONS

1. The Parties agree to designate one or more competent persons to serve as an attorney liaison, and one or more competent persons to serve as a technical liaison for purposes of meeting, conferring, and attending court hearings regarding discovery of ESI, when required.

IV. IDENTIFICATION AND COLLECTION OF HARD COPY DOCUMENTS, ELECTRONIC DOCUMENTS OR DATA, AND ESI

1. The Parties shall meet and confer in an effort to reach agreement on a reasonable list of Custodial Data and Non-Custodial Data sources for purposes of collection, review, and production of Hard Copy Documents, Electronic Documents or Data, and ESI. In connection with the meet and confer process, each Party shall disclose:

i. Custodians. The Individual Custodians likely to have potentially relevant information shall be identified by providing their name, dates of employment, title(s) (if any), and a brief informal summary for the basis of their relevance. The Parties will meet and confer to establish the appropriate number of Individual Custodians to be disclosed based on the complexity, proportionality, and nature of this Litigation.

ii. Non-Custodial Data Sources. A list of Non-Custodial Data sources, if any, likely to contain potentially relevant Documents.

iii. Third-Party Data Sources. A list of third-party data sources likely to contain potentially relevant Documents and, for each such source, the extent to which a Party is (or is not) able to preserve information hosted or stored with any third-party.

iv. Inaccessible Data. A list of data sources, if any, likely to contain potentially

relevant information (by type, date, Individual Custodian or Systems or Database Custodian, electronic system or other criteria sufficient to specifically identify the data source) that a Party contends or asserts is not reasonably accessible under Fed. R. Civ. P. 26(b)(2)(B). In addition to this list, the Parties may agree that certain data sources and ESI do not require preservation by the Parties.

2. The Parties agree that the following data categories shall be deemed inaccessible and therefore, not discoverable, and should not be preserved:

i. 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) and will be collected, searched and produced from those sources if relevant, responsive and non-privileged.

3. The Parties recognize their continuing duty under the Federal Rules of Civil Procedure to disclose Custodial Data and Non-Custodial Data sources in good faith and to supplement their lists of Custodial Data and Non-Custodial Data sources as MDL 3114 progresses when additional sources that contain potentially relevant ESI are located or found without any additional showing of good cause.

4. The Parties agree to meet and confer to discuss the need, if any, for actual or virtual inspection of databases and data systems to develop a discovery plan mandated by Rule 26(f) or to assess how best to collect potentially relevant Documents.

V. SEARCH METHODOLOGY

If the Producing Party elects to use search terms to produce Custodial Data, the Parties

agree to collaborate in as follows:

1. If the Producing Party is identifying or culling potentially relevant materials, the Producing Party shall disclose its identification and culling criteria, including without limitation file type and date restrictions, data sources (including custodians), and other methodologies, employed in assembling a collection to be searched or reviewed.

2. The Parties shall continue to cooperate in testing, evaluating, and revising the appropriateness of any search terms or search term methodology, including:

i. *Producing Party Proposes an Initial Set of Search Terms*: The Producing Party who elects to use a search term process will propose a set of search terms to the Receiving Party.

ii. *Requesting Party's Proposed Revisions*: The Receiving Party will review the search terms list and provide any proposed revisions or additions to the Producing Party's search terms, if any.

iii. *Producing Party Provides Information*: The Producing Party will identify the search terms that it is willing to run and any modifications it is willing to make to its proposed search terms in light of the Requesting Party's proposed revisions.

iv. *Hit Reports:* Upon request, the Producing Party will provide search term hit reports that contain at least the following information: the aggregate hits for each of the disputed terms (i.e., the number of Documents returned by a search term); the number of hits for each term including family members; the number of unique hits for each of the disputed search terms (the number of Documents which contain the particular search term.

v. *Cooperation*: The Producing Party and the Requesting Party will work together in good faith to reasonably and meaningfully narrow the number of documents returned via search term hits and narrow the number of irrelevant documents captured as a result of the

search terms.

3. Upon request, a Party shall not unreasonably decline to disclose pertinent information relating to network and database architecture, database dictionaries and schema, the access control list and security access logging and rights of individuals to access the system and specific files and applications, the ESI 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. Such requests should not be made routinely but only when the information sought is reasonably calculated to support greater accuracy, efficiency or economy in discovery.

4. To the extent that a Producing Party believes that any of the search terms proposed by a Requesting Party are unreasonably overbroad and will result in the identification of disproportionate numbers of irrelevant Documents or undue burden, the Parties will meet and confer to discuss whether the disputed terms should be revised or eliminated from the review and confer in good faith to discuss any additional information or metrics needed to enhance the effectiveness of the proposed search terms.

5. Nothing in this Order will limit a Producing Party's ability to review Documents for relevance or privilege.

VI. USE OF TECHNOLOGY ASSISTED REVIEW (TAR)

1. A Producing Party may not use TAR to cull Documents for production in the absence of a negotiated TAR Protocol. For the avoidance of any doubt, nothing in this Protocol shall prevent a Party from manually reviewing Custodial Data for responsiveness and Privilege.

VII. MATCHING DOCUMENT TO REQUEST

1. For Documents that are produced in a manner not substantially similar to the way in which the Documents are kept in the usual course of business (considering associated metadata

furnished), the Producing Party shall track the request(s) to which such Documents were deemed responsive and shall produce such information in the "ResponsiveTo" field of the data Load File. Should this attribution prove unreasonably burdensome in practice, the parties shall promptly meet and confer to discuss alternative means of attribution, *e.g.,* tying the documents to a limited number of concept clusters or issues, or other suitable alternative.

VIII. DATABASES AND STRUCTURED DATA

1. Prior to collection, the Parties will meet and confer to address the production and production format of any relevant structured data or data contained in databases including cloud-based databases or platforms. Prior to meeting and conferring, the Producing Party will provide information about the database or structured data to the Requesting Party as necessary for the discussion which may include, as applicable: database name; type of database; a list of the fields and field definitions contained within the database; software supporting the database; software version; business purpose; number of users and administrators; size of the database in terms of records; overall size of database in gigabytes (GB) and; a list of standard reports generated by the database.

2. If ESI in a commercial or proprietary database can be generated, provided, or produced in an existing and reasonably usable delimited report format (*e.g.*, Excel, CSV, RSMF), the Producing Party will produce the relevant ESI in such format. If an existing report format is not reasonably available or usable, the Parties will attempt to identify a mutually agreeable format of production based on the specific needs and the content and format of ESI within such structured data source.

3. The Parties shall produce known responsive materials. Documents known to be responsive to document requests shall be produced without regard to whether the files are responsive to any search term, of high "relevance" predicted by a TAR text classification

algorithm, or otherwise flagged as potentially relevant by another search or review methodology. Relevant privileged Documents need not be produced but must be included in an appropriate Privilege Log in accordance with this Order.

IX. MOBILE AND HANDHELD DEVICE DOCUMENTS AND DATA

1. Relevant data on a mobile, handheld, or tablet device shall be produced in a format consistent with the provisions of this Protocol. To the extent relevant data identified on a mobile, handheld, or tablet device is not susceptible to collection or to the production formats set forth in this Protocol, the Parties will meet and confer to address the identification, collection, and production format of any relevant data on mobile, handheld, or tablet devices.

X. FORMS OF PRODUCTION: HARD COPY DOCUMENTS

1. Hard Copy Documents shall be scanned to single page black and white Group IV TIFF format, 300 dpi quality or better with corresponding searchable OCR text as indicated in this Protocol. The Document's original orientation should be maintained (*i.e.*, portrait-to-portrait and landscape-to-landscape). Image file names will be identical to the corresponding Bates numbered images, with a ".tiff" file extension. The file name of each text file should correspond to the file name of the first image file of the Document with which it is associated.

XI. UNITIZING DOCUMENTS

1. In scanning Hard Copy 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, Hard Copy Documents stored in a binder, folder, or similar container should be produced in the same order as they appear in their original container. A scanned version of the front cover of the container should be produced immediately before the first Document in the container. Similarly, the back cover of the container should be produced immediately after the last Document in the container. The Parties and their vendors will

undertake reasonable efforts to logically and correctly unitize Documents and commit to promptly and reasonably address situations of improperly unitized Documents.

XII. HARD COPY DOCUMENT METADATA

1. The following metadata fields should be provided for Hard Copy Documents when reasonably available:

i. Beginning Bates number,

ii. Ending Bates number,

iii. First attachment Bates number,

iv. Last attachment Bates number,

v. Source location/Individual Custodian,

vi. Confidentiality designation,

vii. Redacted (Y/N), and

viii. Extracted/OCR text file path.

XIII. FORMS OF PRODUCTION: ELECTRONIC DOCUMENTS OR DATA, AND ESI

1. The Parties will produce the following forms of Electronic Documents or Data, and ESI in native formats:

i. Excel and other spreadsheet files,

ii. PowerPoint and other presentation files,

iii. Database files,

iv. Delimited text files,

v. Photographs,

vi. Audio and video files, and

vii. Other Documents of a type which cannot be reasonably converted to useful TIFF images as determined by the Parties after meeting and conferring.

2. Documents produced natively shall be produced with the native link (*i.e.*, the link between the native and TIFF file) provided. Each Native file shall be named after its Bates number including any confidentiality designation, and shall have a corresponding ".tiff" placeholder indicating "File Produced in Native Format."

3. All other Electronic Documents or Data or ESI will be produced as single page black and white Group IV TIFF images, 300 dpi quality or better, and 8.5"x11" page size, except for Documents requiring different resolution or page size. The Document's original orientation should be maintained (*i.e.*, portrait-to-portrait and landscape-to-landscape). Metadata to be included, as applicable, is specified in Attachment A.

4. TIFFs of ESI shall convey the same information and image as the original Document, including all comments or commentary, speaker notes, tracked changes (deletions and revision marks, including the identity of the person making the deletion or revision and the date and time thereof), hidden text, embedded Documents or images or other user-entered data, and formatting that is visible in the Native Format version of the file. All hidden content will be expanded, extracted, and rendered in the TIFF file and to the extent possible, the Producing Party will instruct its vendor to force off Auto Date.

XIV. CONFIDENTIALITY DESIGNATIONS

1. Documents designated as "Confidential Information" or "Confidential Attorney Eyes Only Information" shall be so marked in accordance with the Protective Order entered in this Litigation.

2. The Parties will meet and confer regarding instances where the designation cannot be displayed on the face of a Document. Such documents containing Confidential Information or Confidential Attorney Eyes Only Information shall include the appropriate confidentiality designation in the file name. Where possible, the confidentiality designation should also be

included in the metadata of the Document.

XV. PARENT-CHILD RELATIONSHIPS

1. The Parties agree that if any part of a Document or its attachments is responsive, the entire Document and attachments will be produced, except any attachments that must be withheld or redacted and logged based on privilege or work-product protection.

2. The Parties shall take reasonable steps to ensure that parent-child relationships within a Document family (the association between an attachment and its parent Document) will be preserved. 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.

3. Where facilitated by the email system provider (even if requiring a Microsoft 365 supplementary license or a Microsoft 365 upgraded or updated license), the Parties shall collect, search and produce hyperlinked Documents (also known as "Modern Attachments") referenced in responsive Documents. Hyperlinked documents and modern attachments in emails shall, as feasible, be collected, processed and searched in the same manner as embedded (conventional) attachments for the purposes of preserving a family relationship for production. Where it is not technically feasible to collect hyperlinked documents or the family relationship between transmittal and hyperlinked attachment cannot be preserved or readily determined, the Producing Party shall consider reasonable requests for production of hyperlinked documents on a case-by-case basis. For the avoidance of any doubt, the foregoing refers only to linked documents that reside on the producing party's internal systems; under no circumstances shall a producing party be obligated to reconnect links to external sources.

XVI. COLOR

1. Documents that contain color used to convey information (*e.g.*, color coding and highlighting versus merely decorative use) shall be produced as single-page, 300 dpi JPG images with JPG compression set to the highest-quality setting to avoid degrading the utility of the original image.

2. Absent agreement by the Requesting Party, a Producing Party may not use the color version of any file that the Producing Party did not previously produce to the Requesting Party in color. The Parties agree to meet and confer in advance of any hearing or trial to discuss the production of color versions of files included on any exhibit list. Any Hard Copy Documents that are scanned in color shall be produced in color. If a Native file, including but not limited to a PDF, word processing document, spreadsheet, or presentation, is converted to images to effectuate redactions, the redacted version shall be produced in color faithful to the original file.

XVII. FOREIGN LANGUAGE DOCUMENTS

1. All Documents shall be produced in their original language. Where a requested Document exists in a language other than English and the Producing Party also has an English-language version of that Document that it prepared for non-litigation purposes prior to filing of the lawsuit, the Producing Party shall produce both the original Document and all English-language versions. In addition, if the Producing Party has a certified translation of a non-English language Document that is being produced, (regardless of whether the translation was prepared for litigation purposes) the Producing Party shall produce both the original non-English Document and the certified translation. Nothing in this agreement shall require a Producing Party to prepare a translation, certified or otherwise, for non-English language Documents that are produced in discovery.

XVIII. FILE NAMES

1. Each TIFF image should have a unique file name corresponding to the Bates number of that page with a ".tiff" file extension. The file name 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. Bates numbers will be unique across the entire production and prefixes will be consistent across all Documents produced.

2. The Producing Party will brand all TIFF images in the lower right-hand corner with its corresponding Bates number without obscuring any part of the underlying image.

XIX. EXTRACTED TEXT FILES

1. For each Document, a single Unicode text file containing extracted text shall be provided along with the image files and metadata. The text file name shall be the same as the Bates number of the first page of the Document. File names shall not have any special characters or embedded spaces. Electronic text must be extracted directly from the Native electronic file to the extent reasonably feasible unless the Document is an image file or contains redactions, in which case, a text file created using OCR should be produced in lieu of extracted text.

2. Extracted text shall include all comments, revisions, tracked changes, speaker's notes and text from Documents with comments or tracked changes, and hidden and very hidden worksheets, slides, columns, and rows. Text extracted from e-mails shall include all header information that would be visible if the e-mail was viewed in Outlook including: (1) the individuals to whom the communication was directed ("To"), (2) the author of the e-mail communication ("From"), (3) who was copied and blind copied on such e-mail ("CC" and "BCC"), (4) the subject line of the e-mail ("RE" or "Subject"), (5) the date and time of the e-mail, and (6) the names of

any attachments.

XX. LOAD FILES

1. Productions will, as applicable, include image Load Files in Opticon or IPRO format as well as Concordance format data (.dat) files with the applicable metadata fields identified in Attachment A.

2. All metadata will be produced in UTF-16LE or UTF-8 with Byte Order Mark format.

3. Production volumes shall only include one image Load File per production volume. The name of the image Load File shall mirror the name of the delivery volume. The volume names shall be consecutive.

4. All Native Format files shall be produced in a folder named "NATIVE."

5. All TIFF images shall be produced in a folder named "IMAGE," which shall contain sub-folders named "0001," "0002," etc. Each sub-folder shall contain no more than 10,000 images. Images from a single Document shall not span multiple sub-folders.

6. All extracted Text and OCR files shall be produced in a folder named "TEXT."

7. All Load Files shall be produced in a folder named "DATA" or at the root directory of the production media.

XXI. REDACTIONS

1. Any redacted material must be clearly labeled on the face of the Document as having been redacted and shall be identified as such in the Load File provided with the production. Each redaction shall include information identifying the reason for the redaction in the "RedactionReason" field. Each redacted Document shall be produced with an OCR ".txt" file containing unredacted text; the text files should not contain the text of the redacted portions. A Document's status as redacted does not relieve the Producing Party from providing all the metadata

required herein unless the metadata withheld contains privileged content. Nothing herein shall require any Party to create or produce metadata that does not exist or is not reasonably or technically accessible.

2. To the extent that a native spreadsheet must be redacted, the Producing Party may redact the Native file or, if such redaction is not practicable, produce TIFF images with burned in redactions in lieu of a Native file and TIFF placeholder image, provided the TIFF images are reasonably usable. If redacting TIFF images, the Producing Party should make reasonable efforts to cause such images to legibly present all information in the spreadsheet. Nothing herein is intended to override the provisions in section XVI. Color herein.

3. A Party may not redact any Document based upon any objection related to the relevance or responsiveness of a Document. Nothing in this paragraph abridges a Producing Party's right and/or obligation to redact Personal Identifying Information ("PII"), Personal Health Information ("PHI") or sensitive personal information (including, but not limited to, sensitive health information, social security numbers, dates of birth, etc.), provided that the information to be redacted is limited to personal information that is not relevant to the case.

XXII. PRIVILEGE LOGS

1. Within forty-five (45) days of each production (or as otherwise agreed upon), the Producing Party shall supply a log of each Document that has been withheld from production entirely or redacted in part under a claim of privilege and/or work product. The log shall contain sufficient information to allow the receiving Party to understand, evaluate, and test the basis for the privilege claim for each Document. Categorical logs will not be allowed.

2. Privilege logs shall be produced as Excel spreadsheets allowing text searching and organization of data. The privilege log shall include for each withheld or redacted Document a Bates number or other unique privilege log identifier, the type of privilege(s) asserted, all

Individual Custodians of the Document, the date and time of creation or sending, the author or sender, all recipients (separated into primary recipients, courtesy copy recipients, and blind courtesy copy recipients to the extent they are available), and the name of the file or subject line of the e-mail as reflected in the metadata.

3. All attorneys appearing on the log will be identified as such wherever they appear in the log, whether by an asterisk or some other consistent marking or designation. All individuals will be identified by first and last name and e-mail address, wherever they appear in the log, consistent with the information contained in produced metadata. Where metadata, such as the subject line of an e-mail, reflects privileged or protected information, a Party may substitute a description of the Document sufficient to allow Parties to assess the claim of privilege or protection, provided that the privilege log clearly indicates any such substitution. Parties may use reasonable technological processes to identify and log privileged ESI or Electronic Documents.

4. Communications involving external litigation counsel for this case that post-date the filing of the complaint need not be included in a privilege log.

XXIII. DEDUPLICATION

1. The Producing Party will horizontally (globally) de-duplicate only exact duplicate Documents based on the individual file or file family's MD5-Hash, SHA-I hash, e-mail duplicate spare messages (as defined by Relativity), or SHA-256 values at the Document level or by Message ID, or other agreed-upon standard methodology for e-mail deduplication within the collection of an Individual Custodian or a data source in a manner that does not break up Document families (such as e-mails and attachments). Near-duplicate Documents shall not be removed. The original exact duplicate ESI shall continue to be preserved.

2. Attachments to parent Documents may not be deduplicated against a duplicate standalone version if the attachment exists, and standalone versions of Documents may not be

suppressed if a duplicate version exists as an attachment.

3. As to Custodial Data, a Producing Party may de-duplicate globally or only within an Individual Custodian's file, but the produced metadata shall identify each and every Individual Custodian in whose files the Document was found in the "AllCustodians" field. If a Producing Party intends to de-duplicate within Non-Custodial Data, or between Custodial Data and Non-Custodial Data, the metadata provided with the produced Documents shall indicate the other source(s) for the de-duplicated Documents.

4. The Producing Party will track all deduplicated files and provide the names of all Individual Custodians of these duplicates in the load file. If the duplicates are e-mails, the Producing Party must detail the process of creating the Hash Value, *e.g.*, the names and order of concatenated fields by which the deduplication hash was calculated.

XXIV. DE-NISTING

1. System and application files without user-created content (as identified by matching to the NIST National Software Reference Library database) need not be produced.

XXV. E-MAIL THREADING

1. The Parties reserve the right to use email threading to reduce the overall amount of ESI and documents produced and use email thread suppression to avoid review and production of repetitive information contained within an email thread in another document being reviewed and produced *provided however* that email threading shall not serve to exclude any constituent of a thread that would be produced in the absence of threading.

XXVI. PRODUCTION MEDIA

1. The preferred means of production is via secure FTP or secure file share. Productions shall remain available for download for no less than ten (10) calendar days. The Producing Party will retain a copy of all productions made hereunder. Upon request from the

Requesting Party, the Producing Party will make the production available via Secure FTP within two (2) business days of the request.

2. If there is a reasonable concern regarding confidentiality or the size of the production, the Producing Party may use appropriate electronic media (DVD, thumb drive, or hard drive) for its ESI production and will endeavor to use the highest capacity suitable media. The Producing Party will label the production media with the name of the Producing Party, production date, media volume name, and Bates number range(s). Productions on physical media should be encrypted for transmission to the receiving party.

3. At the time of production and under separate cover, the Producing Party shall furnish decryption credentials to the Receiving Party.

4. The Producing Party shall accompany all Document productions with a production cover letter describing by Bates number the Documents being produced.

XXVII. PROCESSING

1. The Parties will use reasonable efforts and standard industry practices to address and resolve exception issues for items that present processing, imaging, or form of production problems (including encrypted, corrupt and/or protected files identified during the processing of ESI). The Parties will meet and confer regarding procedures that will be used to identify, access, process, and resolve any exception issues.

2. Parties shall normalize times and dates to conform to UTC. If a Producing Party cannot process ESI with UTC, the Parties shall meet and confer to determine a reasonable alternative.

3. For archive files (zip, jar, rar, gzip, TAR, etc.), all contents should be extracted from the archive with source pathing and family relationships preserved and produced. The fully unpacked archive container file does not need to be included in the production.

XXVIII. PROCESSING NON-PARTY DOCUMENTS

1. A Party that issues a non-Party subpoena ("Issuing Party") shall include a copy of this Protocol with the subpoena and request that the non-Party produce Documents in accordance with the specifications set forth herein. In the event that the format of a third-party production does not substantially conform with the specifications set forth herein the Parties shall meet and confer regarding how best to address the issue with the producing third party.

2. The Issuing Party is responsible for producing to all other Parties any Document(s) obtained pursuant to a subpoena to any non-Party, in the same form the Document(s) was/were produced by the non-Party. To the extent practical given the data volume and load time, productions by a non-Party should be produced by the Issuing Party to all other Parties within fourteen (14) calendar days of the non-Party's production to the Issuing Party.

3. For the avoidance of doubt, nothing in this Protocol is intended to or should be interpreted as narrowing, expanding, or otherwise affecting the rights of the Parties or non-Parties to object to a subpoena.

XXIX. PRIOR PRODUCTIONS/PRODUCTIONS FROM OTHER PROCEEDINGS

1. Requested copies of production of documents made by a Producing Party in other civil investigations, litigations, and/or administrative actions by federal, state, or local government entities, if relevant to the Litigation, may be provided in the format in which they were previously produced, including any previously produced metadata, load files and accompanying text files, and same Bates numbers and confidentiality designations so long as the Producing Party deems them to be produced in a reasonably usable form as required by Federal Rule of Civil Procedure 34. This paragraph addresses the format of production only and does not impose any obligation to produce documents produced in other proceedings. If the Receiving Party believes that the prior production is not produced in a reasonably useable form as required by Federal Rule of Civil

Procedure 34, the Parties agree to meet and confer and attempt to resolve such concerns on a good faith basis. Notwithstanding Federal Rule of Civil Procedure 34(b)(2)(E)(ii), no party may refuse to reproduce responsive ESI that it has failed to produce in the form or forms requested, in the form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.

XXX. CHALLENGES TO PRIVILEGE CLAIMS OR REDACTIONS

1. Subject to the limitations specified herein, a Receiving Party may timely challenge a Producing Party's privilege claims or redactions. Any Receiving Party disagreeing with a privilege claim or redaction of any Document shall identify in writing the specific Document (identified by bates number or privilege identifier) challenged, and the specific reasons why the challenging Party does not believe the privilege claim or redaction is appropriate and may request in writing that the designating Party remove the claim for privilege or redaction. The designating Party shall then have thirty (30) days after receipt of the written challenge notice to respond in writing and advise the challenging Party as to whether the privilege claims or redactions will be maintained or withdrawn.

2. If the designating Party does not withdraw the claimed privilege or remove redactions from the challenged Documents after expiration of the applicable timeframe set forth above, including any extension of time agreed to by the Parties, and after the conference required under LR 7.1(a) the Parties are unable to reach an agreement regarding the proper designation or redaction of the Document, any Party may seek an order from the Special Masters as to whether the privilege or protection on which the redaction is based applies. If such motion is made, the designating Party bears the burden of establishing that the privilege claim or redaction is proper. The moving Party must seek to file the motion for disclosure under seal in accordance with LR 79.3. In the first instance, the Special Masters will resolve disputes regarding privilege claims or redactions under this Order. If a Special Master determines it would be useful, the Special Master

may ask the Parties for a conference to resolve the dispute informally before the submission of any briefing. If the Parties and the Special Masters are unable to resolve the dispute, they will promptly negotiate and agree to a briefing schedule including page limits depending on the number of Documents being challenged. After briefing is complete, the Special Master will promptly issue an order, report, or recommendation addressing the dispute.

3. A Party may file objections to--or a motion to adopt or modify--the Special Master's order, report, or recommendation no later than twenty-one (21) days from the date that order, report or recommendation is served. Fed. R. Civ. P. 53(f)(2). The Party filing an objection or motion must also file the relevant record if not filed by the Special Master with his order, report, or recommendation. Unless a different schedule is set by the Court, the responding Party must file any written response within ten (10) days after the objection or motion is filed.

XXXI. CLAWBACK

1. Any party who has received a notification of disclosure of protected information from a Producing Party pursuant to the Protective Order, and is not challenging a clawback, shall follow the following procedure to ensure all copies of protected information are appropriately removed from the Receiving Party's system:

i. Locate each recalled document in the document review/production database and delete or sequester the record from the database;

ii. If there is a native file link to the recalled document, remove or sequester the native file from the network path;

iii. If the database has an image load file, locate the document image(s) loaded into the viewing software and delete or sequester the image file(s) corresponding to the recalled documents.;

iv. Apply the same process to any additional copies of the document or

database, where possible;

v. Locate and destroy or sequester all other copies of the document, whether in electronic or hardcopy form. To the extent that copies of the document are contained on write-protected media, such as CDs or DVDs, these media shall be destroyed and rendered unusable or sequestered, except for production media received from the recalling party, which shall be treated as described herein;

vi. If the document was produced in a write-protected format, the party seeking to recall the document shall, at its election, either (i) provide a replacement copy of the relevant production from which the document has been removed, in which case the Receiving Party shall destroy and render unusable the original production media; or (ii) allow the Receiving Party to retain the original production media, in which case the Receiving Party shall take steps to ensure that the recalled document will not be used; and

vii. Confirm that the recall of protected information under this procedure is complete by way of letter or email to the Party seeking to recall protected information.

2. Upon the Parties reaching agreement or resolution that the protected information has properly been clawed back, or the Court's Order sustaining a privilege claim as to protected information, the specific protected information shall no longer be sequestered and shall be permanently deleted.

3. The Parties agree that if a document is used in Litigation and not clawed back by the Producing Party within 120 days, the Receiving Party may challenge the clawback as untimely before the Special Master. The term "used" in Litigation shall refer to documents introduced as

evidence in this Litigation, specifically, marked as exhibits, used in depositions or filed with the Court (as opposed to documents produced to the Receiving Party during discovery).

XXXII. MODIFICATION

1. This Protocol may be modified by a Stipulated Order of the Parties or by the Court for good cause shown.

IT IS SO STIPULATED, THROUGH COUNSEL OF RECORD.

Dated: January 10, 2025

Respectfully Submitted,

/s/ W. Mark Lanier

W. Mark Lanier
THE LANIER LAW FIRM, P.C.
10940 W. Sam Houston Pkwy N.
Suite 100
Houston, Texas 77064
Tel: 713-659-5200
Fax: 713-659-2204
Mark.Lanier@lanierlawfirm.com

Plaintiff's Lead and Liaison Counsel

Shauna Itri
SEEGER WEISS LLP
325 Chestnut Street, Suite 917
Philadelphia, PA 19106
Tel: 215-553-7981
sitri@seegerweiss.com

James E Cecchi
CARELLA BYRNE CECCHI BRODY & AGNELLO PC
5 Becker Farm Road
Roseland, NJ 07068
Tel: 973-994-1700
jcecchi@carellabyrne.com

Jean Sutton Martin
MORGAN & MORGAN
Complex Litigation Group
201 N Franklin St 7th Floor
Tampa FL 33602
Tel: 813-559-4908
jeanmartin@forthepeople.com

Sean S Modjarrad
MODJARRAD ABUSAAD & SAID
212 W Spring Valley Road
Richardson, TX 75081
Tel: 972-789-1664
smodjarrad@mas.law

Plaintiff's Executive Committee

/s/ Gilbert S. Keteltas
Gilbert S. Keteltas
BAKER HOSTETLER LLP
1050 Connecticut Ave., NW,
Suite 1100
Washington, DC 20036
Tel: (202) 861.1530
Fax: (202) 861.1783
gketeltas@bakerlaw.com

C. Shawn Cleveland
Tamara D. Baggett
BAKER HOSTETLER LLP
2850 N. Harwood Street, Suite 1100
Dallas, TX 75201
Tel: (214) 210-1200
Fax: (214) 210-1201
scleveland@bakerlaw.com
tbaggett@bakerlaw.com

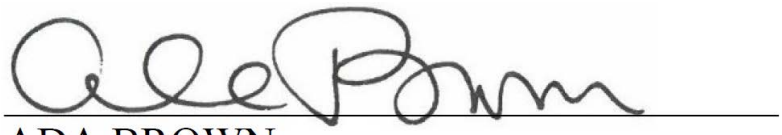
Gregg J. Costa
GIBSON DUNN
811 Main St., Suite 3000
Houston, TX 77002
Tel: (346) 718.6649
gcosta@gibsondunn.com

Attorneys for Defendant AT&T Inc.

/s/ J.T. Malatesta
J.T. Malatesta
POLSINELLI PC
2100 Southbridge Pkwy, Ste. 650
Birmingham, Alabama 35209
Phone: 205.963.7138
Fax: 615.523.2344
JTMalatesta@polsinelli.com

Attorney for Defendant DirecTV, LLC

SO ORDERED this 14th day of January, 2025.



ADA BROWN
UNITED STATES DISTRICT JUDGE

ATTACHMENT A
ESI Metadata

Field Name	Description
BegBates	First Bates identifier of item
EndBates	Last Bates identifier of item
PgCount	Number of pages in the Document
FileSize	Size of native file Document/e-mail in KB.
FileName	Original name of file as appeared in location where collected
Path	E-mail: Original location of e-mail including original file name. Native: Originating path where native file Document was collected including original file name.
NativeLink	Relative path and filename for native file on production media
TextLink	Relative path and filename for text file on production media
AttRange	Bates identifier of the first page of the parent Document to the Bates identifier of the last page of the last attachment "child" Document
BegAttach	First Bates identifier of attachment range
EndAttach	Last Bates identifier of attachment range
AttachCount	Number of attachments to an e-mail
AttachName	Names of each individual Attachment, separated by semicolons
ParentBates	First Bates identifier of parent Document/e-mail message (will not be populated for Documents that are not part of a family).
ChildBates	First Bates identifier of "child" attachment(s); may be more than one Bates number listed depending on number of attachments (will not be populated for Documents that are not part of a family).
Custodian Metadata Field	E-mail: mailbox of the Individual Custodian where the e-mail resided. Native: Individual Custodian from whom the Document originated Systems Data: The name or unique identification of the specific system, or the Systems or Database Custodian, in the event of a production from a system that cannot be associated with a single Individual Custodian.
AllCustodians	Individual Custodians whose file/message has been de-duplicated; separated by semicolons
From	E-mail: Sender Native: Author(s) of Document; separated by semicolons

To	E-mail: Recipient(s); separated by semicolons
CC	E-mail: Carbon copy recipient(s); separated by semicolons
BCC	E-mail: Blind carbon copy recipient(s) separated by semicolons
DateSent (mm/dd/yyyy hh:mm:ss AM)	E-mail: Date and time the e-mail was sent
Subject	E-mail: Subject line of e-mail.
Title	Document: Title provided by user within the Document
MsgID	E-mail: "Unique Message ID" field
Importance	For e-mails, "High," "Low," or "Normal" (or equivalent if an e-mail client other than Outlook was used); Null if no value selected
Sensitivity	For Outlook (or equivalent) e-mails, "Normal," "Private," "Personal," or "Confidential"; Null if no value selected
ReadStatus	Read or Unread
HasAttachments	Indicates that an e-mail has attachments (Y/N)
ModifiedDate (mm/dd/yyyy hh:mm:ss AM)	Document: Last Modified Date and time
CreationDate (mm/dd/yyyy hh:mm:ss AM)	Document: Create Date and time
LastModifiedBy	Person who last modified a Document
FileExt	Document: file extension
FileType	Document: file type
Redacted	Denotes that item has been redacted as containing privileged content (Y/N).
RedactionReason	Identifies the reason for each redaction.
Hash	MD5 Hash value of the item
HiddenContent	Denotes presence of Tracked Changes/Hidden Content/Embedded Objects in item(s) (Y/N)
Confidential	Denotes that item has been designated as confidential pursuant to protective order (Y/N).
DeDuped	Full path of deduplicated instances; separated by semicolons
ResponsiveTo	Identifies the request that the Document is identified as being responsive to