Michael Merriman (SBN 234663)
HILGERS PLLC
mmerriman@hilgerslaw.com
655 West Broadway, Suite 900
San Diego, CA 92101
Telephone: (619) 369-6232

Attorneys for the Plaintiffs and the Proposed Classes

Jeremy Ostrander (SBN 233489)
WHITE & CASE LLP
3000 El Camino Real
2 Palo Alto Square, Suite 900
Palo Alto, CA 94306-2109
Telephone: (650) 213-0300
Facsimile: (650) 213-8158
jostrander@whitecase.com

Attorney for Defendant Experian Information Solutions, Inc.

Elizabeth McKeen (SBN 216690)
Danielle Morris (SBN 246295)
O'MELVENY & MYERS LLP
610 Newport Center Drive
17th Floor
Newport Beach, CA 92660
Telephone: (949) 823-6900
Facsimile: (949) 823-6994
emckeen@omm.com
dmorris@omm.com

Attorneys for Defendant TransUnion

McGregor W. Scott (SBN 142413)
KING & SPALDING LLP
621 Capitol Mall, Suite 1500
Sacramento, CA 95814
Telephone: (916) 321-4818
Facsimile: (916) 321-4900
mscott@kslaw.com

Attorney for Defendant Equifax Inc.

[Additional attorneys on signature page]

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA
SACRAMENTO DIVISION

DR. DERRICK ADAMS, CAPE EMERGENCY PHYSICIANS, P.A., and AMERIFINANCIAL SOLUTIONS, LLC, on behalf of themselves and those similarly situated,

Plaintiffs,

v.

EXPERIAN INFORMATION SOLUTIONS, INC., EQUIFAX INC., AND TRANSUNION,

Defendants.

Case No. 2:23-CV-01773-DJC-JDP

~~[PROPOSED]~~ STIPULATED ORDER REGARDING DISCOVERY OF ELECTRONICALLY STORED INFORMATION

DISCOVERY MATTER

Judge: Hon. Daniel J. Calabretta

Magistrate: Hon. Jeremy D. Peterson

AUTHENTICATED U.S. GOVERNMENT INFORMATION GPO

1. PURPOSE

This Order represents the parties' agreement on technical and other specifications that will apply to discovery of electronically stored information ("ESI") and other documents in this case. This Order shall govern all ESI discovery in this action, as a supplement to the Federal Rules of Civil Procedure and any other applicable orders and rules. It is intended to facilitate efficient, cost-effective discovery, taking into account proportionality, and good-faith cooperation. Nothing in this Order is intended to expand or limit the obligations or privileges of a party or non-party with respect to discovery in this action or as otherwise required by law.

2. DEFINITIONS

Terms used in the Order shall be construed according to the Federal Rules of Civil Procedure and the most recent edition of The Sedona Conference Glossary: eDiscovery & Digital Information Management.

3. SEARCH METHODOLOGY

The parties recognize and agree that each party may use one or more methodologies to identify, search, collect, cull, review, and produce responsive and non-privileged ESI, including the use of keyword search terms, the use of technology assisted review ("TAR"), and/or the use of Artificial Intelligence. The parties agree to meet and confer in good faith regarding document custodians, date range limitations, search terms, and other means of limiting the number of documents requiring collection and review in a manner that is proportional to the needs of the case.

a) Custodians and Data Sources. The parties shall make reasonable efforts to identify and collect documents and ESI from agreed-upon custodial and non-custodial sources that are potentially responsive following a reasonable search. To identify such sources, each Party shall disclose in writing an initial list of its own proposed non-custodial document sources and document custodians. If a Requesting Party contends that additional Custodians or non-custodial sources should be added, then the Parties shall meet and confer in good faith in an attempt to reach agreement. Except by agreement of

the Parties or by order of the Court, a Producing Party is not required to add custodial or non-custodial sources after completion of the above phases.

b) Search Terms. The parties will meet and confer in good faith regarding the search terms to be applied to limit the documents that will be subject to technology-assisted review and/or human review for potential production. The parties shall use reasonable efforts to perform optical character recognition ("OCR") conversion on non-searchable PDF files and other standalone files and email attachments that do not have searchable text in order to make them searchable before applying search terms.

c) Locations not to be Searched. The parties agree, absent a showing of good cause, the following need not be searched or preserved other than as in the normal course of business:

1. Deleted, slack, fragmented, or other data only accessible by forensics.
2. Random access memory (“RAM”), temporary files, or other ephemeral data difficult to preserve without disabling the operating system.
3. On-line access data such as temporary internet files, history, cache, cookies, and the like.
4. Data in metadata fields frequently updated automatically, such as last-opened dates, except as specified in this Order (the metadata fields identified in Appendix A).
5. Back-up data substantially duplicative of data more accessible elsewhere.
6. Voice message systems.
7. Logs of calls made from cellular or landline phones.
8. Mobile devices (e.g., iPhone, Android, and Blackberry devices), including text message and instant message data, unless following reasonable investigation it is discovered that the mobile

device contains unique, relevant, and responsive information that is not available in substance from any other source.

9. Server, system or network logs.

10. Data remaining from systems no longer in use that is unintelligible on the systems in use.

11. Personal digital assistants.

12. Automated disaster recovery backup systems and/or disaster recovery backup tapes.

d) Date Range. The parties will meet and confer regarding the start date and end date to be applied to searches.

4. SCOPE OF PRODUCTION

a) Global De-Duplication. A producing party is only required to produce a single copy of a responsive document. Data shall be globally de-duplicated based on MD5 or SHA-1 hash values at the family level, where possible. Attachments to parents may not be suppressed if a duplicate stand-alone version of the same attachment exists. A "Duplicate Custodian" field containing the identity of each custodian and/or data source that contains a de-duplicated document shall be provided as a metadata field in the production data file. If there are any handwritten notes, or any other markings, on a document, it shall not be considered a duplicate of an unmarked version. Any document that contains an alteration, marking on, or addition to the original document shall be treated as a distinct version, and shall be produced as such.

b) Threading. Each party may de-duplicate email productions in such a way as to eliminate earlier or lesser-included chains of emails. A party may produce only the most complete iteration of an email chain. Any de-duplication tool used by a party must ensure that an email will be suppressed only if its recipients (including CC and BCC recipients), subject, body text (excluding specified automatic footers and normalized to consolidate white space) and attachments are wholly included in another more complete email. If the subsequent most-inclusive message does not include an attachment to an earlier

message, the attachment and its parent must also be produced pursuant to the protocol set forth herein. After receiving and reviewing a party's production, a receiving party may request the production of individual, specifically identified, lesser included portions of a produced email thread. No such reasonable request shall be denied by the producing party.

5. PRODUCTION FORMAT

a) Delivery. Where feasible, productions will be delivered via FTP or other secure file transfer site. Each piece of Production Media shall include a unique identifying label and cover letter including the following information:

- Name of the litigation and its case number;
- Name of the producing party;
- Date of the production (in mm/dd/yyyy format);
- Bates number range; and
- Confidentiality Designation(s).

b) Production Format. All files shall be produced as tagged image file format ("TIFF") images accompanied with an image load file, a data load file, and document-level searchable text.

c) Image Requirements. A TIFF image converted from a native file shall be produced as follows:

- All images shall be Group 4, minimum 300 DPI, single-page TIFF files named according to Bates number.
- With the exception of PowerPoint files (.ppt), which must be imaged in color, a party may choose to produce images in black and white only if color is not necessary to understanding the meaning of the document. A receiving party may request re-production of individually identified black and white documents in color, and no such reasonable request shall be denied by the producing party.

- Hidden content, tracked changes or edits, comments, and other similar information viewable within the native file shall also be imaged so that such content is viewable on the image.
- Bates numbers and any confidentiality designation shall be electronically branded on each produced TIFF image; for documents produced in native format, the Bates number and confidentiality designation shall be electronically branded on the document placeholder and shall not obscure the body of the document.
- 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.
- Each TIFF image shall be assigned a Bates number that is unique and maintains a constant length across the entire document production (i.e., padded to the same number of characters).

d) Production of Native Files. Electronic spreadsheets (e.g., MS Excel files), database or data files (e.g., MS Access or CSV files), photo files (e.g., .jpg, .jpeg, .gif, or .png files) and any document that cannot be readily converted to image files (e.g., audio files, video files, DWG files) shall be produced in native format with an accompanying TIFF placeholder and extracted text file. In the event that a portion of a natively produced file is protected from discovery by an applicable privilege, a party may redact natively or meet and confer as necessary. Each ESI produced in Native Format shall be assigned a unique Bates number, and for each a single-page placeholder, a static image stamped with this unique Bates number, the phrase "Document Produced Natively" (or similar language denoting that the document was produced in native format), and the corresponding confidentiality designation under the Protective Order will be produced. No Party may attach to any pleading or any correspondence addressed to the Court, or any adverse or third party, or submit as an exhibit at a deposition or any other judicial proceeding, a copy of any produced native format document without ensuring that either the corresponding

placeholder slip sheet is attached to the document or the corresponding Bates number and confidentiality legend, as designated by the Producing Party, appears on the document. A party may request that a file produced in TIFF be produced in native if the TIFF omits relevant, substantive content included in the native file or where the TIFF version suffers material, adverse formatting changes as a result of the conversion to TIFF, such as the loss of meaningful color distinctions. PowerPoint files shall be produced with speaker notes visible.

e) Data Load File Requirements. Concurrently with the production of responsive documents, the parties shall produce data load files referencing each document image in the corresponding production, according to the following specifications:

- Images Load File: Opticon (OPT) format.
- Metadata Load File: Concordance-compatible DAT file with field header information added as the first line of the file. Use Concordance default delimiters.
- Extracted Text File: Reference file path to the TEXT file accompanying the TIFF images.
- Native Files Produced: Reference file path to native file.

f) Production of Metadata. Concurrently with the production of responsive documents, the parties agree to produce reasonably available metadata fields identified in Appendix A as part of the production load files. The parties agree and understand that not all metadata information will be available for all types of ESI but otherwise agree to produce reasonably available metadata as outlined below. Although there is no obligation to generate or create metadata not otherwise in existence, the parties agree that certain production-level fields set forth below (e.g., "Custodian") shall be generated during production processing by the producing party's electronic discovery system.

g) Time Zone. Parties shall process ESI in a consistent time zone and identify the time zone used in the TimeZone metadata field in Appendix A.

h) Attachments. The relationship between attachments, enclosures, embedded files, and/or exhibits to any parent document shall be preserved. "Attachments" (also known as "Children") and the documents to which they are attached (the "Parent" document) are a "Family" of documents. Child documents should be located directly after the Parent document in the production set and should be sequentially Bates-numbered. To the extent one or more documents in any family are responsive to any document request, the Parent document and all responsive Children must be produced, excluding any privileged material. Parties shall also produce non-privileged, non-responsive Children if one or more documents in a family are responsive unless the non-responsive attachments contain commercially sensitive information in which case the parties can replace the commercially sensitive, non-responsive document with a slipsheet labeled "Document Withheld as Non-Responsive and Commercially Sensitive." The Parties shall meet and confer prior to producing Non-Responsive slipsheets.

i) Hyperlinked Files. A producing party is not required to collect and produce hyperlinked files unless the data source contains functionality to automatically collect and associate hyperlinked files (e.g., Microsoft Purview, Google Vault) and collection and production is reasonably practical without undue burden. The parties recognize the burden of collecting hyperlinked files and shall meet and confer regarding any other requests for hyperlinked files.

j) Extracted and OCR Text Requirements. The parties will provide electronically extracted text for all produced ESI. The parties will provide OCR text for documents that do not contain electronically extractable text, for redacted documents, and for hard-copy documents. The parties will provide document text as separate, document-level text files not embedded in the metadata load file. The parties will name each text file with a ".TXT" extension and shall name the file the unique Bates number of the first page of the corresponding document.

k) Hard-Copy Documents. To the extent that hard-copy documents are captured within the agreed-to search methodology, each party shall convert all associated

hardcopy documents into electronic images in TIFF format for production. If, due to the format or other circumstances, it is not reasonably possible to convert hardcopy documents into electronic copies, the producing party shall notify the receiving party in writing of the circumstances surrounding such hardcopy documents (including a brief description of the type of document and general subject matter), and the parties shall then confer in good faith to determine the most appropriate means for inspecting or producing such hardcopy documents. Paper documents should be logically unitized for production to the extent reasonably practicable. Therefore, when scanning paper documents for production, distinct documents shall not be merged into a single record and single documents shall not be split into multiple records. Where the documents were organized into groups, such as folders, clipped bundles, and binders, this structure shall be maintained and provided in the load file to the extent reasonably practicable

l) Chat Communications. If a party produces communications from a chat platform, it shall do so in a reasonably usable format. Chat communications include, but are not limited to, corporate communication platforms (for example, Microsoft Teams or Slack), mobile text/SMS messages, and mobile application communications (for example, iMessage, WhatsApp, Telegram, Signal).

m) Database Records and Structured Data. To the extent a discovery request calls for the production of Structured Data, the parties shall be available to meet and confer prior to the production of any source of Structured Data.

n) Other Files. The parties agree to meet and confer in good faith if there are any other file types that encounter difficulties in the production preparation process.

6. CONFIDENTIALITY

Confidentiality of produced documents may be designated in accordance with the Protective Order to be entered in this case.

7. REDACTIONS

A producing party may apply redactions to documents produced in this case to remove (a) privileged information and (b) highly sensitive personal information, including

personal identifiers and medical or health information, and other information subject to protection under applicable law or the Protective Order.

All redactions shall be narrowly tailored and shall not obscure relevant, non-privileged information or render a document misleading. The Parties shall meet and confer regarding any disputes concerning redactions.

8. PRIVILEGE

The producing party will provide a log of documents withheld for privilege containing the following document metadata and information to the extent reasonably available: Document Number, Custodian(s), Author/Sender, Recipient, CC Recipient, BCC Recipient, Date, Email Subject, File Name, and Basis for Withholding (e.g., Attorney-Client Communication, Attorney Work Product). The parties will exchange privilege logs no later than 30 days following substantial completion of document discovery and supplement their privilege logs as necessary thereafter.

A single document containing multiple e-mails in an e-mail chain may be listed on the privilege log as a single entry containing the information from the most recent email in the chain. The Parties are not required to log redacted documents provided they state the reason for the redaction in the text of the redaction box (e.g., Attorney-Client Privilege, Work Product, etc.). The Parties are not required to log privileged documents created after the initiation of litigation in this matter.

9. ESI PROTECTIONS AND PROCEDURES

a) No Waiver of Other Objections. This Protocol shall not imply that discovery requested or produced under the terms of this Protocol is properly discoverable, relevant, or admissible in this or in any other litigation. By entering into this Protocol, the Parties do not waive the right to object to the production of documents on any other grounds.

b) Protective Order. All discovery exchanged pursuant to this stipulation shall be subject to the terms and conditions of the protective order to be entered in this case and nothing in this stipulation shall be construed to modify or amend the provisions of the protective order.

c) Best Efforts Compliance and Disputes. The parties agree to use their best efforts to comply with and resolve any differences concerning compliance with any provisions of this protocol. If a producing party cannot comply in a particular circumstance with this protocol, such party shall promptly inform the requesting party in writing why compliance with the ESI Protocol Order is not reasonable or feasible. No Party may seek relief from the Court concerning compliance or non-compliance with the protocol until it has met and conferred with the other party in a good faith effort to resolve or narrow the area of disagreement.

PURSUANT TO STIPULATION
IT IS SO ORDERED.

Dated: May 8, 2026

JEREMY D. PETERSON
UNITED STATES MAGISTRATE JUDGE

,

Date: May 6, 2026

Respectfully submitted,

/s/ Bennett Rawicki

Bennett Rawicki
(*pro hac vice*)
HILGERS GRABEN PLLC
8750 N Central Expy., Suite 750
Dallas, TX 75231
Telephone: (469) 640-6842
brawicki@hilgerslaw.com

Michael Merriman (SBN 234663)
HILGERS PLLC
655 West Broadway, Suite 900
San Diego, CA 92101
Telephone: (619) 369-6232
mmerriman@hilgerslaw.com

Attorneys for the Plaintiffs and the Proposed Classes

/s/ Jeremy Ostrander

Jeremy Ostrander (SBN 233489)
WHITE & CASE LLP
3000 El Camino Real
2 Palo Alto Square, Suite 900
Palo Alto, CA 94306-2109
Telephone: (650) 213-0300
Facsimile: (650) 213-8158
jostrander@whitecase.com

Robert Milne (*pro hac vice*)
Jack Pace (*pro hac vice*)
Bryan Gant (*pro hac vice*)
WHITE & CASE LLP
1221 Avenue of the Americas
New York, New York 10020
Telephone: (212) 819-8200
Facsimile: (212) 354-8113
rmilne@whitecase.com
jpace@whitecase.com
bgant@whitecase.com

Attorneys for Defendant Experian Information Solutions, Inc.

/s/ McGregor W. Scott
McGregor W. Scott (SBN 142413)
KING & SPALDING LLP
621 Capitol Mall, Suite 1500
Sacramento, CA 95814
Telephone: (916) 321-4818
Facsimile: (916) 321-4900
mscott@kslaw.com

Christopher Yook (*pro hac vice*)
Emily Marsteller (*pro hac vice*)
KING & SPALDING LLP
1700 Pennsylvania Avenue, NW, Suite 900
Washington, D.C. 20006
Telephone: (202) 737-0500
Facsimile: (202) 626-3737
cyook@kslaw.com
emarsteller@kslaw.com

Attorneys for Defendant Equifax Inc.

/s/ Ian Simmons
Ian Simmons (*pro hac vice*)
Patrick Jones (*pro hac vice*)
O'Melveny & Myers LLP
1625 Eye Street, NW
Washington, D.C. 20006
Telephone: (202) 383-5300
Facsimile: (202) 383-5414
isimmons@omm.com
pjones@omm.com

Elizabeth McKeen (SBN 216690)
Danielle Morris (SBN 246295)
O'Melveny & Myers LLP
610 Newport Center Drive
17th Floor
Newport Beach, CA 92660
Telephone: (949) 823-6900
Facsimile: (949) 823-6994
emckeen@omm.com
dmorris@omm.com

Attorneys for Defendant TransUnion

APPENDIX A – METADATA FIELDS

FIELD NAME	DESCRIPTION
BegBates	Beginning Bates number
EndBates	Ending Bates number
BegAttach	Beginning Bates number of the first document in an attachment range
EndAttach	Ending Bates number of the last document in attachment range
Custodian	Name of the custodian or source in possession of the document
AllCustodians	If data was de-duped, list all custodians that had access to the record
FilePath	The full original directory path where the file was stored on the source system at the time of collection
FileName	Original ESI file name
FileExtension	Extension of original ESI file
FileSize	Size of native file document/email in KB
NativeLink	Path to produced native file
EmailSubject	Subject line extracted from an email message
Author	Author extracted from the metadata of a non-email document
From	From field extracted from an email message
To	To or Recipient field extracted from an email message
CC	CC or Carbon Copy field extracted from an email message
BCC	BCC or Blind Carbon Copy field extracted from an email message
DateRcvd	Received date of an email message (mm/dd/yyyy format)
TimeRcvd	Received time of an email message (HH:MM AM/PM format)
DateSent	Sent date of an email message (mm/dd/yyyy format)
TimeSent	Sent time of an email message (HH:MM AM/PM format)
MSGID	Unique message ID generated by email application
DateCreated	Date a file was created (mm/dd/yyyy format)
DateModified	Date the file was last modified (mm/dd/yyyy format)
MD5	MD5 hash value generated by processing tool used for identification of exact duplicate documents
SHA-1	SHA-1 hash value generated by processing tool used for identification of exact duplicate documents
DocumentType	Native or application type of ESI document, for example “Word Document” or “Excel Spreadsheet”
HiddenContent	Indicates presence of hidden properties within ESI document. E.g., Hidden Text, Speaker Notes, Tracked Changes, Hidden Comments etc.
ExtractedText	File path to Extracted Text/OCR File
Confidentiality	Indicates confidential designation under the Protective Order, if applicable
Redactions	Indicates “YES” or “REDACTED” if a document contains redactions
TimeZone	Indicates the time zone of ESI processing.