Managing Electronic Discovery Pitfalls

2022 District of Idaho Eastern Bench-Bar

Conference

Friday, October 7, 2022

I. Overview - The Legal Framework

A. Preservation Obligations

1. Trigger: Parties have an "obligation to preserve evidence from the moment that litigation is reasonably anticipated." *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 269 F.R.D. 497, 521 (D. Md. 2010). This is an objective standard.

    a) For a defendant, the duty to preserve begins no later than the date the complaint is served. *Victor Stanley*, 269 F.R.D. at 522.

    b) For plaintiffs, and often for defendants as well, the duty begins earlier. Examples:

        (1) Text message from plaintiff's CEO to defendants stating "keep it up and you'll find [yourself] in court" for defendants' purported interference with plaintiff's operations triggered duty to preserve, even though text was sent two years before litigation was initiated. *Clear-View Technologies, Inc. v. Rasnick*, No. 5:13-CV-02744-BLF, 2015 WL 2251005 (N.D. Cal. May 13, 2015). Court issued an adverse jury instruction and imposed joint monetary sanctions of $212,320 against defendants for failure to preserve.

        (2) In trade secrets misappropriation case, recently hired employee's e-mail to new employer regarding "potential . . . retaliation" by previous employer triggered employee's duty to preserve even though litigation was not initiated until nearly two years later. *Steves & Sons, Inc. v. JELD-WEN, Inc.*, 327 F.R.D. 96, 106 (E.D. Va. 2018).

    c) But there is no duty to preserve if litigation is merely "a vague or far-off possibility." *Steves & Sons, Inc. v. JELD-WEN, Inc.*, 327 F.R.D. 96, 107 (E.D. Va. 2018).

2. Scope of Preservation

    a) Unless a narrower scope is negotiated, parties must preserve all documents and data that they know or should know are, or could be, relevant to the parties' dispute. *Blue Sky Travel & Tours, LLC v. Al Tayyar*, 606 F. App'x 689, 698 (4th Cir. 2015).

b) Relevant documents are those "likely to have discoverable information that the disclosing party may use to support its claims or defenses." *Victor Stanley*, 269 F.R.D. at 522 (quoting *Zubulake v. UBS Warburg LLC (Zubulake IV)*, 220 F.R.D. 212, 217–18 (S.D.N.Y. 2003)).

c) Courts analyze a party's compliance with the duty to preserve based on a standard of "reasonableness under the circumstances." *Victor Stanley*, 269. F.R.D. at 522.

3. Possession, Custody or Control

a) Fed. R. Civ. P. 34(a)(1) provides that a party may serve a request within the scope of Rule 26(b) for production of documents within the responding party's "possession, custody or control."

b) The key word is "control." ("Possession" and "custody" are generally regarded as narrower concepts.) Parties "must preserve potentially relevant evidence under their 'control.'" *Victor Stanley*, 269. F.R.D. at 523.

c) The definition of "control" varies among jurisdictions.

(1) At its most narrow, control means "the legal right to obtain the documents upon demand." *Dugan v. Lloyds TSB Bank, PLC*, No. 12-cv-02549-WHA (NJV), 2013 WL 4758055, at *2 (N.D. Cal. Sep. 4, 2013); (quoting *In re Citric Acid Litigation*, 191 F.3d 1090, 1107 (9th Cir. 1999)). This standard has been adopted in the Ninth Circuit and several other federal circuits.

(2) Other circuits have interpreted control more broadly to mean the "practical ability" to obtain the documents at issue. *See, e.g., Shcherbakovskiy v. Da Capo Al Fine, Ltd.*, 490 F.3d 130, 138 (2d Cir. 2007).

(3) In either case, "control" may include certain documents within the possession of third parties, such as corporate affiliates, agents, and employees. *See, e.g., Puerto Rico Tel. Co. v. San Juan Cable LLC*, No. CIV. 11-2135 GAG/BJM, 2013 WL 5533711, at *1 (D.P.R. Oct. 7, 2013) (defendant's duty to preserve extended to the personal e-mail accounts of defendant's former officers). But the duty to preserve documents controlled by third parties differs among jurisdictions. *See Victor Stanley*, 269. F.R.D. at 523-24 (discussing preservation obligation differences among federal circuits).

B. Perils of Noncompliance

1. Federal Rule of Civil Procedure 37 provides a range of possible sanctions for failing to make disclosures or to cooperate in discovery.

2. Federal Rule 37(e) was revised in 2015 and specifically addresses failure to preserve ESI:

   a) Text: "If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve the information, and the information cannot be restored or replaced through additional discovery, the court may: (1) Upon a finding of prejudice to another party from loss of the information, order measures no greater than necessary to cure the prejudice; (2) Only upon a finding that the party acted with the intent to deprive another party of the information's use in the litigation, (A) presume that the lost information was unfavorable to the party, (B) instruct the jury that it may or must presume the information was unfavorable to the party; or (C) dismiss the action or enter a default judgment."

   b) Key points:

      (1) No strict liability for a party's inability to produce ESI. "The rule recognizes that 'reasonable steps' to preserve suffice; it does not call for perfection." Fed. R. Civ. P. 37(e) advisory committee's note to 2015 amendment; *see also Marten Transp., Ltd. v. Plattform Advert., Inc.*, No. 14-CV-02464-JWL-TJJ, 2016 WL 492743, at *4 (D. Kan. Feb. 8, 2016).

      (2) The court may order a producing party to search for duplicates from other sources, such as back tapes ("information cannot be restored or replaced through additional discovery"). If ESI can be restored or replaced from such sources, curative measures and sanctions are not available.

      (3) The court may order curative measures upon a finding of prejudice if ESI is lost. Curative measures may include any measures except for those set forth in Fed. R. Civ. P. 37(e)(2) (e.g., striking pleadings, denying introduction of evidence, allowing evidence or argument on the failure to preserve).

(4) Mere negligence is not sufficient for adverse inference or adverse judgment ("intent to deprive"—rejecting Second Circuit's holding in *Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99 (2d Cir. 2002)).

(5) However, proof of prejudice is not required—as it was in all circuits prior to the rule revision—as a prerequisite for issuance of an adverse inference, dismissal, or default judgment. The advisory committee's comments note that prejudice may be inferred by a finding of intent. (*Compare Markstrom*, 294 Or App at 344 ("To properly exercise discretion to impose the sanction of dismissal, the court must consider more than the egregiousness of the conduct being sanctioned. . . . The court had to consider the effect of plaintiff's conduct in the context of the case as a whole, including whether and to what extent it prejudiced defendant and, if prejudice to defendant was not an issue, why that was not significant in the context of this case.").

(6) Provides courts with the option to issue one of three severe evidentiary sanctions when the court finds there has been an "intent to deprive" another party of discovery."

(7) The rule only applies to ESI. Spoliation of paper documents may be subject to a different standard, depending on the circuit and the court.

(8) As always, local rules may differ.

(9) The advisory committee's notes call for courts to consider "the party's sophistication with regard to litigation in evaluating preservation efforts; some litigants, particularly individual litigants, may be less familiar with preservation obligations than others who have considerable experience in litigation." Fed. R. Civ. P. 37(e) advisory committee's note to 2015 amendment.

(10) The advisory committee also recognized that the scope of the preservation obligation may not be clear at the outset of a dispute and cautioned that "[i]t is important not to be blinded to his reality by hindsight arising from familiarity with an action." Fed. R. Civ. P. 37(e) advisory committee's note to 2015 amendment.

c) Even where an adverse inference or adverse judgment is not warranted, monetary sanctions may be imposed. *See, e.g.*, *Exp.-Imp. Bank of Korea v. ASI Corp.*, No. CV162056MWFJPRX, 2018 WL 3203038, at *5 (C.D. Cal. June 28, 2018) (awarding defendants monetary sanctions for plaintiff's deletion of hard drive and other e-discovery failures, but declining to award evidentiary sanctions under Fed. R. Civ. P. 37(e) because defendants were not irremediably prejudiced and plaintiff lacked intent to deprive defendants of information).

3. Other bases for sanctions

a) Fed. R. Civ. P. 16(f) – Authorizes sanctions, including a reasonable attorney's fees, for failure to prepare for scheduling conferences and failure to cooperate in pre-trial orders.

b) Fed. R. Civ. P. 26(g)

(1) Mandates sanctions for improper certifications by counsel concerning discovery disclosures, requests, responses, and objections.

(2) The sanctions "may include an order to pay the reasonable expenses, including attorney's fees, caused by the violation." Fed. R. Civ. P. 26(g)(3).

(3) In *Rodman v. Safeway Inc.*, No. 11-CV-03003-JST, 2016 WL 5791210, at *3 (N.D. Cal. Oct. 4, 2016), the court awarded plaintiff $688,646 in attorney fees under Rule 26(g) due to defendant's failure to conduct a reasonable search during discovery of a computer drive, which, when searched shortly before trial, resulted in the discovery of 10 highly relevant documents.

c) Court's inherent authority

(1) Broad in scope in that it "extends to a full range of litigation abuses." *Chambers v. NASCO, Inc.*, 501 U.S. 32, 46 (1991).

(2) But litigant must have "engaged in bad-faith conduct or willful disobedience of a court's orders." *Id.* at 47.

4. Spoliation of Non-Traditional ESI:

a) *Olney v. Job.com*, No. 1:12-CV-01724-LJO, 2014 WL 5430350 (E.D. Cal. Oct. 24, 2014): Court issued adverse inference instruction against plaintiff in response to deletion of web browsing history.

b) *Brown v. Tellermate Holdings Ltd.*, No. 2:11-CV-1122, 2014 WL 2987051 (S.D. Ohio July 1, 2014): Court imposed an issue preclusion sanction for defendants' failure to preserve relevant information stored in the cloud on Salesforce.com. Even though defendant's counsel had issued a "general directive" to preserve relevant information, neither defendant nor its counsel took meaningful follow-up steps to ensure preservation.

C. Proportionality

1. Federal Rule of Civil Procedure 26(b) was revised in 2015 to elevate the importance of proportionality in discovery. The rule now requires courts to consider six factors in assessing proportionality:

   a) The importance of the issues at stake in the action;

   b) The amount in controversy;

   c) The parties' relative access to relevant information;

   d) The parties' resources;

   e) The importance of the discovery of resolving the issues; and

   f) Whether the burden or expense of the proposed discovery outweighs its likely benefit.

2. No Oregon equivalent. As one potential avenue for arguing proportionality under Oregon law, the following was taken from a footnote in a motion for protective order filed by Karen O'Connor and Melissa Healy in *Otnes v. PCC Structurals, Inc.*, Case No. 16cv32466:

   a) The scope of a party's requested discovery must be proportional to the claims or defenses at issue. *Cf.* FRCP 26(b)(1) ("Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case * * *."); *see also Lindell v. Kalugin*, 353 Or 338, 297 P3d 1266 (2013)

3. Key takeaways from recent cases addressing challenges to the scope of discovery in light of new Rule 26(b)(1):

a) Parties should not rely on cases applying earlier versions of Rule 26(b)(1) because those cases were "effectively abrogated" by the rule change. *In re Bard IVC Filters Prod. Liab. Litig.*, 317 F.R.D. 562, 564 (D. Ariz. 2016); *see also Fulton v. Livingston Fin. LLC*, No. C15-0574JLR, 2016 WL 3976558, at *8 (W.D. Wash. July 25, 2016) (sanctioning defendant's counsel for citation to cases analyzing preamendment Rule 26).

b) Courts are more inclined to reject discovery requests that on their face appear overly broad.

c) Parties must now be prepared to thoroughly address proportionality in discovery motion practice, including providing evidence to support or rebut claims that discovery sought is not proportional. "[I]nput from both sides" is essential. *Bard*, 317 F.R.D. at 564.

4. *Odeh v. City of Baton Rouge/Parish of E. Baton Rouge* No. CV 14-793-JJB-RLB, 2016 WL 1254361 (M.D. La. Mar. 29, 2016): Plaintiff asked his former employer to produce his entire e-mail inbox from the time that he was with the company: 2001 through 2014. The inbox contained 64,685 messages. Defendant objected that it was unreasonable and disproportionate to require it to do a privilege review of all of those messages, when most of the messages would unquestionably not be relevant to the claims in the case. The court agreed, holding that the plaintiff needed to identify the subject matter of the e-mails being requested, and that asking for an entire container of information was, in this instance, not proportional.

5. *First Niagara Risk Mgmt., Inc. v. Folino*, 317 F.R.D. 23 (E.D. Pa. 2016): The court concluded that broad discovery—including imaging of entire devices—was proportional. *First Niagara* involved claims for breach of fiduciary duty and theft of trade secrets against a former executive who allegedly started a competing company while employed by First Niagara. The company demanded that the executive turn over his personal and business devices for imaging and searching using key terms; the executive resisted on several grounds including cost and intrusion into his private business. The court went through the multi-factor analysis called for in the rules and found that, on balance, plaintiff's needs outweighed the harm to defendant, and that defendant's proposed limited search protocol was "inadequate." Importantly, the court rejected defendant's argument—made with some basis in the case law—that a responding party should presumptively be permitted to make the first pass at responding to substantive requests, finding that principle to have been modified by the federal rules' emphasis on proportionality.

6. *In re Bard IVC Filters Prod. Liab. Litig.*, 317 F.R.D. 562 (D. Ariz. 2016): The plaintiffs sought extensive discovery from defendants' foreign subsidiaries' communications with foreign regulators. Applying the new Rule 26 factors, the judge (who was chair of the Advisory Committee at the time of the rule changes) first noted the parties' errors in relying on cases applying the pre-2015 rules, because those cases were "effectively abrogated" by the rules change, and made the case that under the new rules, proportionality is given equal standing with relevancy in determining the scope of discovery. The court agreed that plaintiffs' requests were not highly relevant, in that there were no foreign plaintiffs, and plaintiffs could not back up their suspicion of a "smoking gun" in the foreign communications. The court also agreed that the requests were not proportional, because of the expense to defendant of locating, collecting, translating and reviewing communications from 18 countries.

7. *Cargill Meat Solutions Corp. v. Premium Beef Feeders, LLC*, No. 13-cv-1168-EFM-TJJ, 2015 WL 3937410 (D. Kan. June 26, 2015): The court applied the proportionality guidance under the old rules, but in a manner similar to the analysis used in the new rules. The court found that plaintiff had not substantiated its objection to discovery merely by putting forward evidence about the cost of the discovery sought. The court criticized plaintiff for not comparing that cost to the amount in controversy, or for providing support for its cost estimate.

II. Practical Tips for Managing Electronic Discovery

A. Overview

1. Electronic discovery is discovery. It is part and parcel of every litigated matter in state court, federal court, or arbitration.

2. The comments to ABA Model Rule 1.1 (same as ORPC 1.1), concerning attorney competence, require attorneys to "keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology." In litigation, this necessarily means that attorneys should have familiarity with e-discovery practices (or should be able to associate with attorneys who have such competence).

3. Courts expect the senior trial lawyer to be familiar with and be able to defend decisions about preservation, collection, review, and production.

4. Developing and following a consistent e-discovery protocol for each case is essential to avoiding problems.

5. In most complex litigation matters, it is important to engage an electronic discovery vendor such as Streamline Imaging early in the process. Vendors provide invaluable assistance in streamlining the e-discovery process and assisting with compliance, information governance, policies and procedures, data mapping, and defensible deletion, among other things.

6. Confer with opposing counsel early on issues like the form of production / file types, search terms, custodians, anticipated problems, etc. Bring in the court as necessary.

7. Each stage of the e-discovery process requires careful planning and attention to detail.

    a) *See* Exhibit 1 for a depiction of the e-discovery process.

    b) *See* Exhibit 2 for a master checklist of issues to consider in the e-discovery process.

B. Stage 1: Identification

1. To assist the client with issuing an effective preservation notice/legal hold, it is important to understand what electronic sources may contain relevant information, and who may have generated or stored relevant information.

2. Understand the Client's Electronic Systems

a) Attorneys must have a thorough understanding of how the client stores data, what sorts of data deletion practices and policies the client employs, and where relevant data may reside.

b) If the client is a business or other type of organization, arrange to speak with a member of the IT department or with someone knowledgeable about IT.

c) Consider the types of electronic data that the client maintains and whether they may be relevant to the matter. Possible sources include:

(1) E-mail

(2) Network file servers and shared network files

(3) Individual PCs

(4) Personal storage (e.g., hard drives, thumb drives, optical discs)

(5) Tablets and phones

(6) Backup tapes/systems

(7) Voicemail

(8) Text messages

(9) Calendar data

(10) Cloud storage

(11) Social networking sites (e.g., Facebook, LinkedIn)

(12) Chat and instant message programs (e.g., Slack, WhatsApp)

(13) Proprietary systems used for communications and document sharing

(14) Third party sources (e.g., vendors that maintain client data, corporate subsidiaries of a client, contractors)

(15) Data stored on personal devices used by client employees

d) Key questions to ask include:

(1) What protocols exist relating to preservation or destruction of electronic data?

(a) Is there an archiving, auto-delete, or other "janitorial" function associated with any electronic storage or applications?

(2) What types of e-mail systems and accounts are in use?

(a) Consider both personal and business/organizational e-mail accounts.

(3) What types of computer systems are in use?

(a) Is there a central network server?

(b) Can data be saved to local workstations?

(c) Obtain a list of any operating systems, software, and hardware in use that may contain relevant data.

(4) Does the client use cloud-based storage that may contain relevant data?

(5) Does the client store data on removable media, such as CDs, thumb drives, or external hard drives?

(6) What sort of backup systems are in place?

(a) Physical media backup? (e.g., backup tapes and hard drives)

(b) Cloud-based backup services?

(7) What methods of electronic communication does the client use other than e-mail?

(a) Text messages (including iMessage and similar message formats)?

(b) Instant message applications (e.g., Facebook messenger, MS Link, Google Chat)

(c) Are text messages or instant messages saved to iCloud or a similar application?

(8) Does the client maintain a website or use social media?

(9) What other internet-connected products does the client use that may contain relevant data? Newer sources of potentially discoverable data include Amazon Echo devices and similar products.

3. Identify key custodians—the individuals likely to have relevant information.

    a) Preliminary identification of custodians should be done by consulting with the client shortly after intake.

    b) In connection with the preservation directive/legal hold process, prepare (or advise the client to prepare) a custodian survey (*see* Exhibit 3) and ask custodians to complete, sign, and return it.

    c) Interview key custodians to follow up on the questionnaire.

    d) Prepare a custodian data inventory (*see* Exhibit 4). This will be important for collection and for discussions with vendors.

4. Approach the identification process with a skeptical eye.

    a) Do not expect the people you interview to know the law. Clients often have their own understanding of relevance that may be narrower than the legal definition. As a result, clients may not always disclose a source or a category of documents if they do not think it is relevant.

    b) Particular care must be taken in working with clients who are not technologically sophisticated or are unfamiliar with the litigation process. Treat the identification stage as if you were conducting cross examination of a witness in a deposition.

5. Identification sets the stage for all subsequent steps.

    a) Identification is necessary to issue an effective legal hold.

    b) Identification helps to reveal the scope and particulars with respect to document collection.

    c) Identification helps in preparing for negotiations with opposing parties (e.g., is the ESI "reasonably accessible" under Fed. R. Civ. P. 26(b)?).

6. Always memorialize your interviews in writing. This will allow you to retrace your steps and will ensure you are better prepared for discovery battles.

C. Stage 2: Preservation

1. As noted above, the potential consequences of not preserving are serious, and can include monetary sanctions, adverse inference instruction, even judgment against your client. The following steps do not necessarily need to be done in the order in which they are presented, and not every sub-step below will be warranted in every case. At every step, it is critical to document what actions were taken, and if an action was not taken, why not.

2. First step: advise the client regarding a preservation directive, a/k/a a litigation "hold".

   a) A litigation hold is a communication issued as a result of current or reasonably anticipated litigation, audit, government investigation or other such. It can (and should) be issued early and updated as needed.

   b) Counsel should memorialize advice concerning the need for a litigation hold in a memo or letter to the client. (*See* Exhibit 5.) The litigation hold should detail the role of outside counsel in creating, implementing, and monitoring the hold.

   c) The litigation hold must be customized to fit the case and the client's particular situation. Some clients have sophisticated protocols in place to distribute a litigation hold in every case; this does not mean, however, that outside counsel has no role in the litigation hold process.

   d) *See* Exhibit 6 for a sample litigation hold memorandum.

   e) Elements of a litigation hold:

      (1) Assumes that all documents related to the issues in dispute will be subject to discovery or used to defend against a claim of spoliation;

      (2) Encompasses paper document and tangible things, as well as ESI;

      (3) Briefly describes the litigation or matter;

      (4) Explains the recipient's obligation to preserve;

      (5) Describes the subject matter of the documents and data that need to be preserved (and a date range if applicable);

(6) Describes the types and possible locations of data to be preserved;

(7) Provides in-house contact information to field any questions or concerns;

(8) States the duration of the hold (generally until further notice from counsel);

(9) Requires that the recipient acknowledge receipt, in writing; and

(10) Is distributed to all custodians and all other individuals or groups who have control over data sources (e.g., IT departments).

3. Second step: advise the client regarding implementing and monitoring the hold.

a) Consider whether forensic collection of some ESI may be necessary in order to ensure preservation.

(1) Some data sources are difficult to reliably preserve without collection. Examples include databases, smartphones, social media sites, dynamic websites, and third-party hosted data sources. Discuss with the client whether those data sources are potentially implicated and implement a "collect to preserve" protocol for those sources.

b) Monitor and track how the litigation hold is being disseminated and to whom.

c) Work with the client's IT department to ensure preservation of data. Key issues to discuss with IT include:

(1) Suspending routine document destruction protocols and ensuring that auto-delete/janitorial functions are turned off

(2) Ensuring that backup tapes/drives are taken out of rotation/not overwritten

(3) Ensuring that IT is maintaining a record of the devices/sources that are being preserved

(4) Whether to create a snapshot/backup outside of the regular process for preservation purposes and/or to use for collection.

d) Advise and assist client with sending reminder hold notices at regular intervals.

e) Consider whether it is necessary to change the hold (expanding or narrowing it) as the litigation progresses.

f) Failure to implement a litigation hold adequately may subject the client and the client's attorneys to monetary sanctions and adverse inference instructions.

g) Advise the client regarding lifting the hold once litigation has ended and preservation of documents is no longer required because litigation is no longer reasonably anticipated.

4. Third step: issue a document preservation demand to adverse (and potentially adverse) parties.

a) These are serious documents; courts have referred to pre-litigation preservation demands in ruling on spoliation motions.

b) The demand should specify in detail what types of documents you expect will be preserved.

c) *See* Exhibit 7 for a sample preservation demand letter.

d) Consider negotiating an agreement with opposing counsel at an early stage. The agreement can address limitations on the scope of preservation. The agreement can also involve a clawback agreement (FRE 502) regarding privileged documents.

e) Some courts have their own template/default form of agreement. Check local rules and standing orders. Note that the District of Oregon has a model protective order, but it does not include a clawback provision. Even in a case where there is no applicable model order, consider proposing that the parties use another court's model order as a template for negotiation.

D. Stage 3: Document Collection

1. Document collection is the process of gathering data for processing and review.

2. Collection (and processing) can be expensive. Therefore, before you move to the collection stage, it is important to assess short-term objectives and strategies with the client.

a) Is this a case that might settle in the short term? If so, collection/processing may end up being unnecessary.

b) However, it may be necessary to review some documents in order to properly advise the client on settlement.

c) Striking the proper balance between saving on e-discovery and potentially remaining in the dark on the content of documents should be considered carefully.

3. Also consider timing. Collection, processing, review, and creation of a production file all take time – usually more time than one would anticipate. Anticipating deadlines and working backwards, early collection is often advisable.

4. Strategic Collection Methodologies

a) Strategic/targeted collection may reduce e-discovery expenses by reducing the volume of ESI the needs to be processed and reviewed. There are several ways to limit the collection of data, including by using keyword lists, custodian limiters, and date ranges.

b) Some methods of filtering out data are not available at the collection stage, and may only be performed at the "pre-processing" or "culling" stage at a lower cost/burden. What methods are available depends on the type of data being collected.

c) Although not always possible, collection methods ideally will be the subject of negotiation with your opponent before the collection takes place.

d) If the collection is being done after a request for production has been received, it may be easy to target the collection to only documents covered by the request. However, it is frequently difficult to determine what documents are responsive to a request, making the use of search terms or other methodology necessary. Because re-doing a collection is (usually) more expensive and burdensome for the client than re-doing culling, filtering or searching on data that has already been collected, it will frequently be to the client's advantage to collect *broadly,* and then rely on pre-processing to cull the universe of data using keywords/search terms, or other limiters.

5. Who performs the collection?

a) The client? An outside vendor? A mix? The answer will depend on the particulars of each case.

b) Issues to consider regarding who performs the collection:

(1) The type of case and role of the custodians. Some courts have held that "self-collection" is impermissible if the person doing the collection has a personal interest in the outcome of the case. For example, in an employment case it would not be advisable to allow the plaintiff's manager to collect her own data. Clients should be carefully counseled about the risks of self-collection.

(2) The volume of data being collected.

(3) The number and type of sources from which data is being collected.

(4) Whether some of the collection needs to be forensically sound.

6. Performing a Forensically Sound Collection

a) Proper collection of ESI utilizes tools and process that preserve the integrity of the data, including file metadata.

b) Metadata is data that describes the characteristics of ESI, such as how, when and by whom ESI was collected, created, accessed, modified, and how it is formatted. Altering metadata may make document filtering and searching more difficult, if not impossible. It will also result in a production to the other side that may not comply with the applicable civil rules of procedure. For that reason, use of collection methods that will not preserve critical document metadata is generally not advisable and should not be done without discussing the form of production with opposing counsel.

c) In most instances, a forensically-sound collection will require the services of a vendor with appropriate credentials. However, forensic remote collection and even self-collection tools are becoming increasingly available.

d) Tools exist for collection of almost all data in native or near-native format, but some sources pose special challenges.

(1) In some instances, such as performing a forensically sound collection from mobile devices, forensic tools may be required (e.g., EnCase, FTK).

(2) Data from internet or intranet sources, including websites, social media, SharePoint, SAAS tools, and cloud-based databases, also typically require the services of a vendor to conduct a forensically sound collection.

(3) Be particularly careful with webmail; self-collection is difficult and data can easily be lost if not handled correctly.

e) Generally, the more complex the project, the more an outside vendor's involvement in collection should be considered.

7. Data privacy laws/cross-border issues

a) When dealing with clients who may have documents within their control in foreign countries, it is important to be cognizant of applicable local laws.

b) Many countries, particularly countries in the European Union as well as Japan, have stringent data privacy laws, sometimes called "blocking statutes." The EU Data Protection Act, for instance, is very broad. It prohibits personal data (data relating to a natural person who can be identified by the data) from being exported into the U.S. unless an exception applies.

8. Documentation is critical.

a) Maintain (or make sure the vendor is maintaining) meticulous chain of custody records and a collection log of all ESI collected. Be sure to include:

(1) When and how data was collected or received

(2) From whom (which custodian), and where

(3) The volume of the data

(4) Where the data is being stored and/or processed

b) Document any decisions made with respect to collection, including any "targeted collection" techniques.

E. Stage 4: Data Processing

1. Once data is collected, it needs to be processed before it can be loaded into review software such as Relativity. Processing will usually take place in phases.

2. The first phase involves "ingesting" data into software to perform "pre-processing" or "culling."

3. Pre-processing/culling is often used to reduce the volume of data to be "promoted" into full processing and may include some or all of the following steps:

    a) Filtering using keyword search terms, date restrictions, and custodians.

    b) File-type filtering and de-NISTing (removing known system files that will not contain relevant data)

    c) De-duplicating

        (1) Removes identical documents from a data set when the two documents possess identical characteristics, regardless of file name. Can reduce data set by 50%, depending on characteristics of the data universe, with resultant savings in review time.

        (2) Relies on an algorithm that generates a unique value for every file (similar to DNA), called the "hash" value.

        (3) Documents will only "de-dupe" if they are identical in every way. A change to a comma or a piece of metadata will result in two distinct files that will not "dupe out."

        (4) De-duplication can be done in different ways, and there are risks associated with each method. The method of de-duplication should be considered as a topic for discussion with the opponent.

4. Processing may include some or all of the following:

    a) Extracting attachments and metadata from native files

    b) Converting from native to TIFF images

    c) Unitization (the process of combining individually scanned pages into documents)

    d) OCR'ing data for files that do not contain searchable text

    e) Creating a "load file" that can be loaded into a review platform, such as Relativity, DMX, Concordance, or CaseLogistix.

5. Text analytics can also be applied to streamline the review process. Analytics tools include the following:

a) E-mail threading: Detects and organizes separate e-mail documents that are part of a single chain or conversation family.

b) Near-duplicate detection: Identifies and groups nearly identical documents, such as multiple versions or drafts of the same document.

c) Foreign language identification: Groups documents with the same foreign language together for review by translators or reviewers fluent in that language.

d) Clustering and similar-document analysis: Goes beyond keyword searching to group conceptually similar documents together.

6. Advanced analytics - Technology Assisted Review ("TAR" a/k/a Predictive Coding)

a) TAR uses an algorithm to rank documents by relevance based on human review of a small sample set.

b) Typical steps include the following:

(1) ESI is collected and organized via traditional methods. If appropriate, keyword searches and de-duplication is applied.

(2) A subject-matter expert (typically a more senior attorney) reviews a sample set of documents and codes the documents based on relevancy.

(3) Following the initial sample set review, the subject-matter expert continues to review small samples of documents to further train the system. This creates a confidence index, allowing the reviewer to say with a degree of statistical confidence that the documents are accurately coded.

(4) The system applies the human reviewer's coding to other documents at a rate of approximately 150,000 documents per hour and codes them on a sliding scale from most to least relevant.

(5) The case team reviews the results, performs QC spot checks, and makes decisions about further review based on the particular needs of the case.

c) Benefits: Fast, accurate, and cost effective in identifying responsive and potentially key documents in a large volume set (particularly greater than 100,000).

d) Limitations:

(1) Not as useful or cost-effective when dealing with a small number of documents for review.

(2) Not as useful for identifying privilege documents.

(3) Not as useful when a document set contains a large number of relevant or responsive documents that will need to be reviewed by human reviewers at some point.

e) TAR is now widely accepted as a defensible means of reviewing documents to comply with discovery requests.

(1) "The case law has developed to the point that it is now black letter law that where the producing party wants to utilize TAR for document review, courts will permit it." *Rio Tinto PLC v. Vale S.A.*, 306 F.R.D. 125, 127 (S.D.N.Y. 2015) (Peck, M.J.).

(2) There is a growing consensus that the same standard applies to TAR that applies to other methods of review. Judge Peck noted that "it is inappropriate to hold TAR to a higher standard than keywords or manual review. Doing so discourages parties from using TAR for fear of spending more in motion practice than the savings from using TAR for review." *Rio Tinto PLC v. Vale S.A.*, 306 F.R.D. 125, 129 (S.D.N.Y. 2015) (Peck, M.J.); *see also Dynamo Holdings Ltd. P'ship v. Comm'r of Internal Revenue*, No. 2685-11, 2016 WL 4204067, at *6 (T.C. July 13, 2016).

(3) The determination regarding how to comply with discovery requests is still up to the responding party. Absent a showing of deficiency, the responding party cannot be forced to use predictive coding. *Hyles v. N.Y. City*, No. 10CIV3119ATAJP, 2016 WL 4077114, at *2-3 (S.D.N.Y. Aug. 1, 2016).

f) It is advisable to confer with your opponent regarding the use of predictive coding. It may also be advisable to enter into a stipulation to memorialize the parties' understanding regarding the use of predictive coding. *See* Exhibit 8 for a sample predictive coding agreement.

F. Stage 5: Review & Analysis

1. Document review and analysis is frequently the most expensive component of e-discovery, because it often involves manual or linear review of documents by attorneys or other legal professionals.

2. Mistakes can be made during the review process that may be difficult to correct later. Taking time to plan the review workflow carefully can prevent mistakes and save money for the client.

3. Issues to consider:

   a) Who performs the review?

   b) How many levels of review will you be employing?

   c) What is the goal? Review goals may include production to your adversary, identification of helpful documents, tagging documents according to particular issues, identifying privileged documents or documents containing confidential information.

      (1) How should the tagging protocol be structured in the electronic review database to meet immediate as well as long-term needs of the case?

      (2) If your review calls for the identification of "hot documents," it is important to provide reviewers with detailed instructions and examples of what to look for. Consider using specific issue tags.

   d) Will you need to create a privilege log?

      (1) If so, consider including tags for privilege descriptions as part of your review protocol that will allow you to auto-populate the log by exporting information from tags.

      (2) Consider discussing with your opponent what types of information the log should include.

4. When using a document review team that includes people outside of the "core" case team, it is a best practice to have a written document review protocol to provide to team members, along with in-person training before review begins. The written review protocol should include:

    a) An overview of the case, substantive issues in contention, and particular concerns or issues about the data set being reviewed;

    b) A list of tags and the procedure for tagging documents—common tags include responsive, non-responsive, privileged, for redaction, hot, question/follow up, language (for foreign language docs), and confidential;

    c) Examples of important/hot documents;

    d) Documents that are required reading (e.g., complaint, requests for production, etc.);

    e) Instructions and examples regarding privilege and confidentiality issues, including a list of individuals and entities whose communications may be privileged;

    f) A protocol for posing questions about responsiveness and privilege;

    g) Instructions for redacting documents; and

    h) Deadlines.

5. Particularly when a review team is being used, it is important to perform quality control checks early and often.

G. Stage 6: Production

1. Production forms:

    a) Production of ESI is often done in the form of a "load file" that includes Bates-numbered TIFF images, along with metadata.

    b) Requests for production in native format only are becoming more common, but can complicate Bates numbering and confidentiality designations.

    c) Production of file types that do not lend themselves to conversion to TIFF format (e.g., spreadsheets, PowerPoint presentations, Word documents with track changes and comments, audio/video files) is typically done in native format only.

2. The form of production should be discussed at the Rule 26(f) conference or in a meet and confer. If there are problems with a requested format, create a paper trail of your efforts to resolve the dispute.

3. Creating a production file takes time. Depending on the complexity of the production, it may take 48 hours or more to complete all of the necessary processing steps and generate a production file that can be delivered to your opponent.

4. Spot check and verify the contents of a production before it goes out the door. Check the Bates numbering and wording of any confidentiality legends required by a protective order or statute.

5. Maintain a production log.

H. Requesting Documents

1. Fed. R. Civ. P. 34(a) expressly provides that a party may request production of ESI and that the requesting party may specify the form of production. IRCP Rule 34 provides the same and states that "if no such specification is made, the responding party must produce the information in either the form in which it is ordinarily maintained or in a reasonably useful form."

2. Your document requests should specify not only what you want, but how you want it.

   a) Provide detailed instructions concerning the form of production of ESI. Consider the specifications for metadata and items that will be necessary to receive a "load file" that works with the review platform that has been selected. Those specifications may have been a topic of discussion at the Rule 26(f) (or equivalent) conference. Because technology and requirements change, do not rely on production specifications used in prior requests for production.

   b) For sample instructions to specify the form of production, *see* Exhibit 9.

   c) Consider requesting document retention policies and protocols, posing questions about systems architecture, and asking for policies on employee storage of ESI, in order to assess compliance with your requests for production or set up lines of inquiry at deposition about compliance with discovery obligations.

III. Important Litigation Events & Topics Involving E-Discovery

A. The Rule 26(f) Discovery Conference

1. Fed. R. Civ. P. 26(f) requires parties to confer and plan for discovery at the outset of the case. Whether or not a discovery planning conference is required by rule or local practice, it is often a useful practice, particularly in complex cases or if you anticipate needing a specific type of ESI based on the specifics of a case (*e.g.*, old security videos, QuickBooks files, Snapchat, etc.). Consider pushing to have such a conference in every case.

2. The Rule 26(f) conference is intended to prompt the parties to discuss, among other things, initial disclosures required under Rule 26(a)(1), preservation of evidence, form of production, and development of a proposed discovery plan.

3. Issues to consider discussing during the conference (*see* Exhibit 10 for a comprehensive list):

    a) Particulars of preservation and categories of documents to preserve;

    b) The scope of ESI relevant to the lawsuit, including what needs to be searched/collected/produced;

    c) Use of a protective order/clawback agreement;

    d) Filtering methodologies including keyword searching, de-duplication, and other collection/review limiters;

    e) Form of production (technical specifications);

    f) Potential methods for expediting discovery, including phased discovery or rolling productions;

    g) Review requirements and protocols, including use of predictive coding or other non-linear review methods;

    h) Third-party discovery;

    i) Other ways to reduce the cost of discovery.

4. If evidence preservation or other technical issues have already arisen and are highly likely to be discussed at the Rule 26(f) conference, consider having a third party e-discovery vendor attend or help in preparing for the conference.

B. Stipulated Protective Orders

1. A protective order entered by the court is a fairly standard item in complex litigation. Usually the parties negotiate a protective order when they are concerned about keeping documents confidential and want to bind the other parties to a confidentiality protocol. Usually the protocol will give a producing party the ability to stamp a document "confidential," bar receiving parties from distributing such a document outside of the litigation team, and require a receiving party to ask the court to accept the document under seal if it needs to be used in the litigation.

2. The protective order can also be used to limit the cost and burden of e-discovery. The protective order can provide that if a privileged document is produced in discovery, the producing party is entitled to demand that the document be returned and any copies made by the receiving parties destroyed. This is referred to as a "clawback" agreement.

3. A clawback agreement is particularly useful in cases involving large volumes of e-mail. The volume of e-mail that is often involved in complex litigation increases the chances that a privileged e-mail will slip through and be produced, even if the e-mail is going through a linear review.

4. Under FRE 502, parties may agree that privileged documents must be returned upon demand regardless of whether the producing party took "adequate" steps to avoid production. Most importantly, FRE 502 provides that if such an order is entered by the court, the right to claw back the document is binding on all subsequent litigation in federal or state court. Under some circumstances the client may decide to forgo a privilege review entirely and rely on the ability to clawback privileged documents under a FRE 502 agreement. This may reduce the costs of review siginficiantly.

5. Note that sample/model protective orders such as those issued by the District of Oregon may not include the necessary language to provide the full protection that FRE 502 offers.

6. *See* Exhibit 11 for a sample protective order with an FRE 502 clawback agreement.

C. The Corporate Representative (Fed. R. Civ. P 30(b)(6) Deposition

1. Corporate representatives will sometimes be requested to testify regarding preservation, collection and production of documents.

2. Careful preparation is required if this will be one of the topics of inquiry for our client's deposition. Consider having a separate witness designated to handle these topics.

3. If you suspect that your opponent has not adequately searched for responsive documents, consider using a corporate representative deposition to investigate whether the opponent has complied with its discovery obligations.

4. *See* Exhibits 12 and 13 for issues and sample questions to be used at a deposition of a corporate representative regarding e-discovery issues.

D. Using ESI for Summary Judgment or Trial

1. Special care is required when using ESI for summary judgment or trial. Both hearsay and authenticity issues can often come up when ESI is used, and some courts have excluded evidence on those bases.

2. Kirkpatrick, Oregon Evidence has a thorough discussion of authenticating different types of evidence, including emails and website screenshots. Rule 901: "The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."

   a) Note that "Even if an email is successfully authenticated, it is not admissible to prove the truth of its content unless an additional foundation is laid showing that it fits an exception to the hearsay rule." Kirkpatrick at 963

      (1) Admission of a party opponent

      (2) *Sea-Land Serv. V. Lozen Int'l, LLC*, 285 F.3d 808 (9th Cir. 2002) (treating a forwarded email as an adoptive admission)

      (3) *State v. Cunningham*, 179 Or App 359, 378 n 8 (2002) (noting possibility that an email may be admissible as an excited utterance), *rev'd on other grounds*, 337 Or 528 (2004).

   b) *Perfect 10, Inc. v. Cybernet Ventures, Inc.*, 213 F Supp 2d 1146, 1154 (C.D. Cal. 2002) (in copyright case, declarations that printouts were "true and correct" copies of internet pages, "in combination with circumstantial indicia of authenticity (such as the dates and web addresses)" would support a reasonable juror belief that documents are what proponent claims).

c) *United States v.* Jackson, 208 F.3d 633, 637 (7th Cir. 2000) (website postings were offered to prove truth of matter asserted and therefore needed to satisfy hearsay exception)

3. *United States v. Safavian*, 435 F. Supp. 2d 36 (D.D.C. 2006) dealt with the issue of authentication of e-mail for trial:

a) ESI may be self-authenticating under FRE 902(11) via FRE 803(6) Business Records Exception

b) Alternately, ESI may be authenticated under FRE 901(a) upon a showing that there is sufficient evidence "to support a finding that the matter in question is what its proponent claim." This requirement can be satisfied with evidence of "[t]he appearance, contents, substance, internal patterns, or other distinctive characteristics of the item, taken together with all the circumstances." FRE 901(b)(4). Emails typically contain distinctive characteristics, such as the "@" symbol. *Safavian*, 435 F. Supp. at 40.

c) Laird C. Kirkpatrick, Oregon Evidence, Sixth Edition, cites *Safavian* as exemplary of "most modern cases."

4. *Lorraine v. Markel Am. Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007) dealt with authentication of email for summary judgment:

a) The court excluded exhibits that had not been properly authenticated, including emails. The emails were simply attached as exhibits to summary judgment motions.

b) The court's decision discusses the many ways in which ESI may be authenticated under FRE 901 and 902.

c) Most frequent ways to authenticate emails:

(1) FRE 901(b)(1) (person with personal knowledge)

(2) FRE 901(b)(3) (expert testimony or comparison with authenticated exemplar)

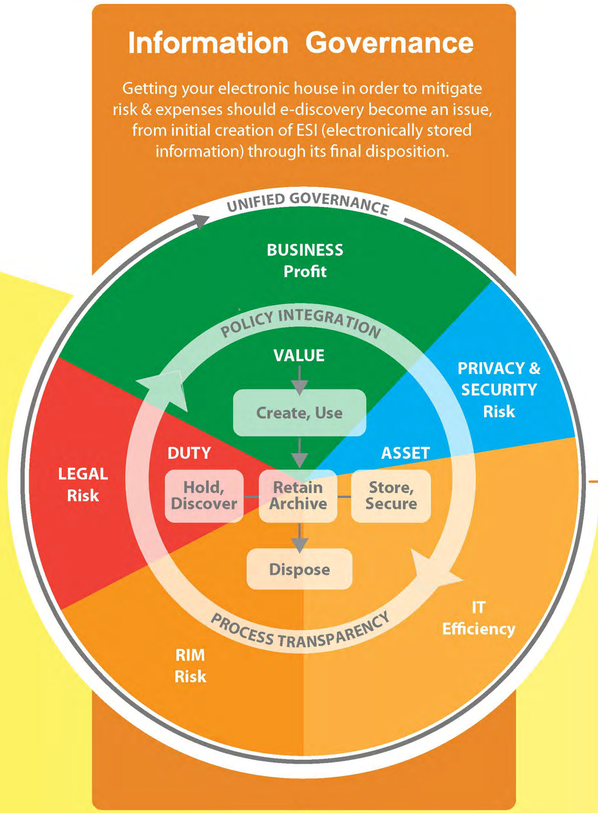
(3) FRE 901(b)(4) (distinctive characteristics, including circumstantial evidence),

(4) FRE 902(7) (trade inscriptions)

(5) FRE 902(11) (certified copies of business records)

Electronic Discovery Reference Model

Standards, Guidelines, and Practical Resources for Legal Professionals and E-Discovery Practitioners



Identify
Locating potential sources of ESI & determining its scope, breadth & depth.

Preserve
Ensuring that ESI is protected against inappropriate alteration or destruction.

Collect
Gathering ESI for further use in the e-discovery process (processing, review, etc.).

Process
Reducing the volume of ESI and converting it, if necessary, to forms more suitable for review & analysis.

Review
Evaluating ESI for relevance & privilege.

Analyze
Evaluating ESI for content & context, including key patterns, topics, people & discussion.

Produce
Delivering ESI to others in appropriate forms & using appropriate delivery mechanisms.

Present
Displaying ESI before audiences (at depositions, hearings, trials, etc.), especially in native & near-native forms, to elicit further information, validate existing facts or positions, or persuade an audience.

VOLUME

RELEVANCE

Electronic Discovery Reference Model

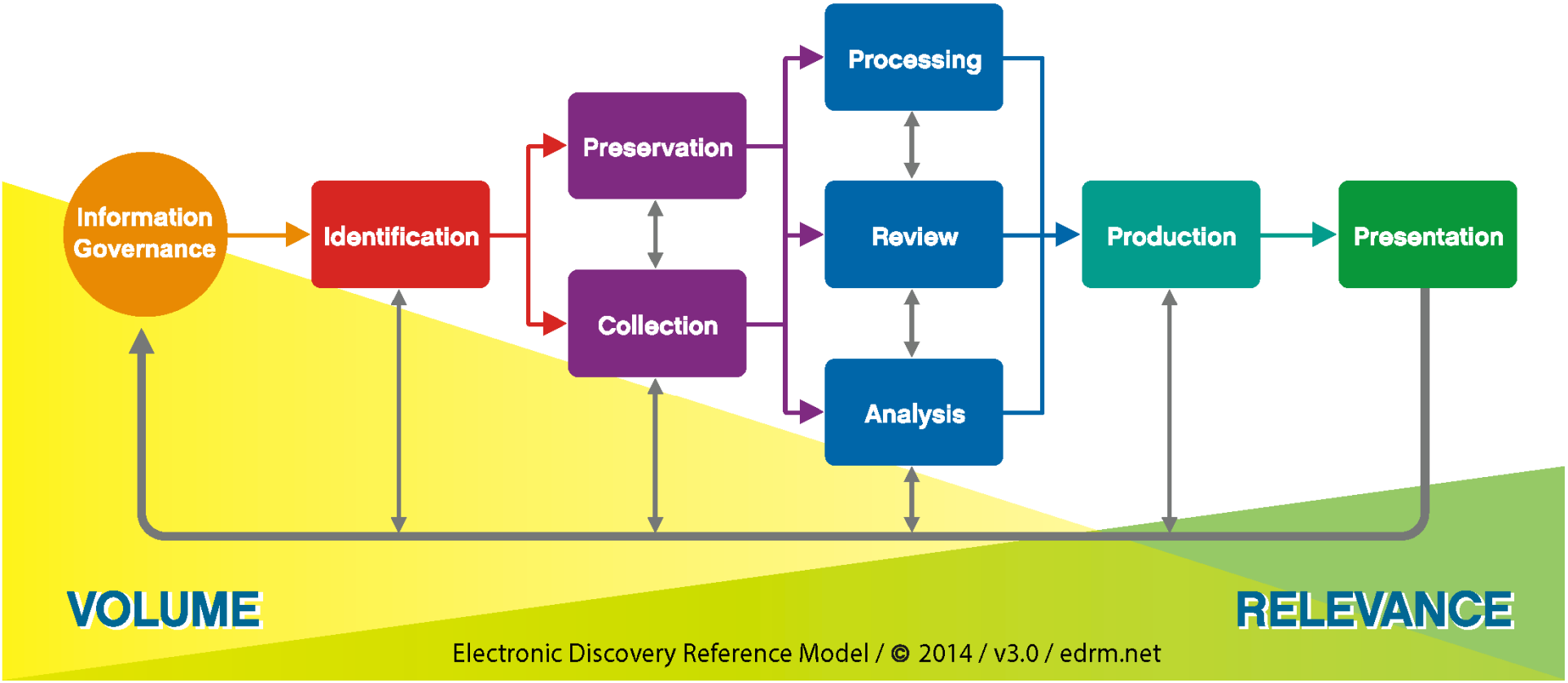


Exhibit 1

Master Checklist For Discovery

☐	Work with client to identify sources that may contain relevant information and custodians likely to have generated or stored relevant information.
☐	Advise the client regarding instituting, implementing, and monitoring a litigation hold; memorialize advice in writing. Consider whether immediate collection is necessary to preserve.
☐	Issue a preservation demand to adverse (and potentially adverse) parties.
☐	Discuss discovery matters with the opposing party during discovery planning conference.
☐	Consider negotiating a clawback agreement (FRE 502) with opposing counsel to address the inadvertent production of privileged documents.
☐	Develop a plan to perform a targeted collection of documents from the client. Decide what needs to be collected and from whom, as well as who will perform the collection – including consideration of whether outside vendor assistance is necessary.
☐	Consider complications that may result from foreign data privacy laws in performing the collection.
☐	Ensure that relevant data has been collected and processed for review.
☐	Determine whether it is necessary to restore deleted ESI or obtain data from backup systems.
☐	Request documents from the opposing party and from third parties.
☐	Serve any objections to the opposing party's document requests.
☐	Meet and confer with the opposing party regarding discovery disputes.
☐	Consider discovery motion practice, including motions for protective orders, motions to compel, and motions for forensic inspections.
☐	Develop a plan to conduct the document review. Consider issues such as the goals of the review, the volume of data at issue, costs, and similar factors.
☐	Supervise document review and perform quality control on review.
☐	Discuss a production schedule and the procedures for production with the opposing party. Consider a stipulated protective order.
☐	Produce documents and maintain a production log.

ATTORNEY-CLIENT PRIVILEGED AND CONFIDENTIAL

CUSTODIAN SURVEY

TO: Custodians

FROM: [Attorney name]

Please fill in the information requested below and return the original to [name] as soon as possible. **Please do not make any copies, scan, or e-mail this document to anyone. If you should have any questions regarding this document, please contact [name] by phone.**

Name: _____ Office Location: _____

Phone: _____ Job Title: _____

***Description of legal matter*:**

[Insert]

You have been identified as a custodian of potentially relevant documents (including but not limited to electronic and paper copies of documents and drafts of those documents, and communications of every type, including e-mail, text messages, and voice mail) in connection with this matter. In order to ensure that [client] fully complies with its legal obligations, you are required to fully and completely answer the below questions relevant to your personal practices and policies with regard to creation and storage of potentially relevant documents.

In this questionnaire, your work-issued desktop or laptop computer is referred to as your "Main Computer."

If you have any questions about any of the terms used in this questionnaire, please CALL [name]; do not send an e-mail.

1. Please describe the responsibilities of your current position.

2. Please identify any assistant, secretary, or other personnel working directly for you or with you that may have potentially relevant documents.

3. Do you currently use a computer other than your Main Computer while you are working in the office?

   If yes, please provide information (i.e., brand, usage, work performed, accessible to others, location, etc.) about that computer.

4. Since [date], have you used a computer different than your Main Computer to work remotely?

   If yes, please provide information (i.e., brand, usage, work performed, accessible to others, location, etc.) about the computers that you have used.

5. Since [date], have you used a home computer for work purposes?

   If yes, please provide information (i.e., brand, usage, work performed, accessible to others, location, etc.) about home computers that you have used.

6. From [date] to the present have you used any computer (other than those identified in response to prior questions) to create, review, revise, or store potentially relevant documents?

   If yes, please provide information about any computer that you no longer use, including any information that you have concerning the whereabouts of that computer(s).

7. Since [date], has your Main Computer or the hard drive on your Main Computer changed?

   If yes, please provide information on the location of your prior Main Computer or the prior hard drive(s) of your Main Computer.

8. Please describe each method that you have used since [date], to access work-related e-mail and computer files while you are out of the office (e.g., Outlook Web Access, VPN, Citrix, BES, smart phone, laptop, etc.).

9. Since [date], have you used an e-mail account other than your [client] e-mail account, including e-mail accounts on an Internet or cloud-based service (e.g., Gmail, Hotmail, Yahoo, America Online, etc.) for work purposes?

   If yes, please provide information about those accounts including the (1) e-mail addresses used; and (2) dates of usage.

   If yes, please also identify all devices or computers that were used to access such e-mail accounts.

10. Since [date], have you ever created your own archive to store e-mail or stored e-mail in a location other than on the [client] e-mail system?

    If yes, please identify all locations where you stored or saved those archives or e-mails.

11. Since [date], have you used any program other than MS Windows to delete files?

    If yes, please identify the program(s) used, and provide information regarding what was deleted and when it was deleted.

12. Since [date], have you stored any work-related documents or e-mails on your Main Computer's hard drive ("C:" drive)?

    If yes, please list all locations (e.g. folders) on your Main Computer's local hard drive that you have used for that purpose.

13. Please list all locations on the [client] shared file servers where you may have stored potentially relevant documents since [date].

14. Since [date], have you used any kind of instant messaging application or program, on any device, to create or review a message that may be considered a potentially relevant document?

    If yes, please list: (1) any instant messaging applications or programs used; and (2) identify the device(s) on which the application or program was used.

15. Since [date], have you used any external storage media (e.g., "floppy" disks, CDs, DVDs, USB devices, "flash drives," "thumb drives," external hard drives, etc.) to store work-related documents or communications?

    If yes, please provide: (1) information about the location of those pieces of external storage media; and (2) the information that was stored on such media.

16. Since [date], have you used your personal digital assistant or smartphone (e.g., Blackberry, Palm Pilot, iPhone, etc.), tablet computer, or any other mobile device other than a computer identified above, to create, review, revise, or store potentially relevant documents?

    If yes, please provide all information about any such device(s) including the current location of any device that you no longer use.

    If you have any potentially relevant data on a mobile device that you believe may not exist in the company's system, please immediately call [name] at [phone number].

17. Since [date], have you used encryption (e.g., PGP, EFS, TruCrypt, etc.) on any computer or device that you have listed above?

    If yes, please list the application(s) used and identify each device on which the encryption application(s) was used.

18. Since [date], have you used any applications to compress computer files (e.g., Zip, Tar, Rar, etc.) on any computer or device that you have listed above?

    If yes, please identify the application(s) used and identify each device on which the compressing application(s) was used.

19. Since [date], have you utilized any kind of "cloud-based" storage for work-related material (e.g., iCloud, Dropbox, Google Drive, Box, etc.)?

    If yes, please list: (1) the storage service(s) that you have used; and (2) the nature of the documents stored in those locations.

20. Since [date], have you made any notes or created, reviewed, revised or stored any potentially relevant documents—electronic or paper—that were not stored on your local hard drive, the [client] shared network drive, in e-mail, or in any other storage location that you have identified in response to a question above?

    If yes, please provide information about: (1) where the document(s) is currently stored or was stored; and (2) the nature of the document(s).

21. Since [date], have you saved any voice messages that may be considered relevant documents?

    If yes, please identify where such messages were saved.

22. Since [date], have you experienced any loss of or destruction of potentially relevant documents, whether because of physical loss of a data storage device or computer, or because of a software "crash" or some other cause relating to software?

    If yes, please provide information regarding the loss or destruction.

PLEASE RETURN THE ORIGINAL OF THIS SURVEY
TO [NAME] VIA HAND DELIVERY ONLY.
IF YOU HAVE ANY QUESTIONS, PLEASE CALL [NAME].

Electronic Discovery - Custodian Data Inventory

Custodian	Email Accounts	Shared Network File Sources	Databases	Personal Computers / Laptops	Phones/Tablets	Other Physical Storage (e.g., hard drives, optical discs, thumb/flash drives)	Cloud Storage	Social Media Accounts (e.g., LinkedIn, Facebook, Twitter, Instagram)
Sample: John Doe	jdoe@clientx.com jdoe@gmail.com	Client H drive iManage Worksite	Concordance	Workstation - Dell Optiplex 960 Home Computer - Apple iMac	Samsung Galaxy S6 Apple iPad Air 2	Portable 500GB Seagate HDD Two 8 GB flash drives	Google Drive Account Apple iCloud Account	Facebook: jdoe5533 LinkedIn: jdoe5533 Twitter: @jdoe5533

Exhibit 4

Memorandum

ATTORNEY-CLIENT PRIVILEGED

To: CLIENT
From: ATTORNEY
Subject: Preservation of Potential Evidence/Litigation "Hold"
Date: DATE

I. Introduction

This memorandum follows up on our prior discussions about preservation of evidence and the above [litigation/describe matter].

As you are aware, [opponent] has [describe litigation or potential litigation], concerning [describe subject matter], in [describe court or jurisdiction] ("the litigation"). Courts have become increasingly exacting in requiring the preservation of both paper documents and electronically stored information ("ESI") that may be relevant to litigation. Generally, upon either reasonable anticipation of litigation or actual notice of litigation, a party has a duty to take affirmative steps to preserve all potentially relevant evidence. In this regard, it is imperative that you comply with the [Federal Rules of Civil Procedure/insert other applicable rules] and take immediate steps to preserve relevant evidence, including ESI. This memo provides legal advice to you with regard to preservation of hard-copy information and ESI, and outlines our recommendations as we move forward. How to go about *collecting* documents/information for use in the litigation will be the subject of additional communications, if necessary.

As you may know, the litigation process may involve discovery, including demands from the other side that documents and other information be produced. The [Federal Rules of Civil Procedure/insert other applicable rules] define the scope of the documents and information that may be subject to discovery *very* broadly. In particular, the term "document" is defined to include much more than the “final version” of a document. Instead, the term encompasses all forms of ESI and hard-copy materials, and includes drafts of such materials.

Thus, when we discuss documents or information in this context, it is important to remember that we are in fact referring to what we traditionally think of as documents (reports, letters, spreadsheets, hand written or typed notes, etc.) in hard copy or electronic form, and also drafts of such documents, as well as *all forms* of ESI located on your computer network, hard-drives, back-up tapes or drives, portable storage, or any other type of electronic storage media (including cloud-based storage or storage maintained by third parties). The scope of the preservation obligation extends to all documents and information under your custody *or* control. This means that your documents that are in the custody of others should be the subject of preservation efforts. The scope of preservation even extends to personal or home devices, if those devices may contain information that is potentially relevant to this matter.

II. Your Preservation Obligation & Our Role as Outside Counsel

A. You Have An Obligation to Preserve Evidence.

Courts have imposed serious sanctions against parties who permit evidence to be destroyed or lost, even if the destruction is

inadvertent. These sanctions have included monetary penalties and default judgment.

As a general rule, a party's obligation to preserve potentially relevant records, including ESI, for purposes of litigation arises when the party has notice that the evidence is relevant to litigation or when a party should reasonably know that the evidence may be relevant to future litigation. **The preservation obligation has been triggered in this case.** Since the obligation has been triggered, you must institute a discovery management plan.

[insert further recommendations regarding discovery management plan, if applicable]

B. Outside Counsel Is Required to Be Involved In Evidence Preservation.

Courts have held that a party and its outside and in-house counsel must take additional "affirmative steps" to ensure that a party meets its electronic discovery obligations during all phases of litigation. Specifically, courts have held that outside counsel must take an active role regarding the institution and monitoring of efforts to preserve evidence. Cases from courts around the country have confirmed that it is imperative that outside counsel work closely with the client to ensure that potentially relevant information is preserved.

The courts have imposed several distinct duties upon outside counsel in connection with preservation of potentially discoverable information, be it in electronic or paper form. These duties apply to us. They include the following:

- Counsel has a duty to communicate effectively to you your discovery obligations so that all relevant information is preserved, and so that all

relevant, non-privileged information may later be produced. This memorandum will satisfy that requirement.

- When the duty to preserve attaches, and where the client supervises other people who may have relevant documents counsel (or you, under counsel's direction) must put in place an internal preservation directive (litigation hold). In order to ensure that the directive is disseminated to the appropriate personnel, counsel must (either itself or through your representative) identify sources of discoverable information, such as that in the possession of key company personnel or in the possession of IT staff.
- Counsel (or you at counsel's direction) must reiterate the hold instructions on a regular basis.
- Counsel must actively monitor the instructions and, when needed, corrective action must be taken to ensure continued compliance.

Fulfilling these obligations is not simply a matter of avoiding sanctions for you or for us. Following the procedures recommended in these cases will also save time and money in litigation. The [Federal Rules/insert applicable rules] now require that counsel meet and confer at an early stage about, among other things, discovery of electronic (and hard-copy) documents. Outside counsel's task in preparing for this conference ([referred to in the Federal Rules as the "Rule 26(f)" conference/insert reference to provision in other applicable rules]) is made much easier if proper steps are taken at the preservation stage to investigate the sources of potentially relevant information.

C. What Must be done to Preserve Relevant Information

1. *Identify custodians*: Prior to issuing any preservation directive, it is essential to correctly identify all personnel who may possess or be in control of relevant information. Identify the employees, representatives and/or agents of the company with information or knowledge related to the litigation (the "custodians" or "key players"), relevant business units, departments and archives of stored data;

a. Based on the information that we currently have, the relevant custodians appear likely to be, at a minimum: [INSERT WHAT IS KNOWN ABOUT CUSTODIANS]

b. **We are required to work with you to identify additional custodians**. Additional custodians will be people who have or had access to documents concerning the following topics: inspection of operations for compliance with environmental permits.

2. *Identify physical locations*: Identify the physical locations of hard-copy documents (e.g. the "job file") and of servers, hard drives and other electronic storage devices that may hold electronic information, including locations that may not be readily accessible, such as data residing on backup media or systems. **We are required to work with you to determine the locations of information to be preserved, if there is any question as to what locations contain information to be preserved.**

3. *Distribute a written preservation directive (aka "litigation hold")*: A preservation directive must be distributed to all custodians identified as potentially having information that must be preserved, *and* those responsible for the physical

locations identified above (such as individuals within your Information Technology (IT) department. The preservation directive must direct custodians and IT to disable or modify any retention policies or practices to ensure preservation of all potentially responsive data and records in the company's possession, custody or control. The preservation directive can come from us or from you. You should be aware that some courts have held that the preservation directive is not protected from disclosure by the attorney-client privilege. [A sample/suggested preservation directive is attached.]

In connection with distribution of the preservation directive we further recommend that each custodian be given a written questionnaire to obtain further information about the information that each custodian may have generated or stored. [A sample/suggested custodian questionnaire is attached.] The preservation directive and custodian questionnaire should also attempt to determine if any data (e.g. old email) may have already been destroyed pursuant to an internal policy or practice.

4. *Discuss the preservation obligation with IT*: It is essential that your information technology (IT) staff confirm that they understand the scope of the preservation obligation and that they have taken appropriate steps to disable janitorial functions that may result in information being lost. As part of our obligations as outside counsel we are required to ensure that IT has been consulted, either by participating in the discussion with IT directly or confirming with you that IT has been consulted.

5. *Document your preservation efforts*: Maintain written records of all steps taken to preserve data, including with respect to (1) sources of evidence, including ESI, that are subject to preservation, (2) the distribution of hold notices, (3) and discussions that take place with IT and relevant custodians.

6. *Repeat*: Remind custodians and IT personnel regularly of their preservation obligations.

During the course of the litigation we will be required to continually re-evaluate the custodian list and the scope of your preservation obligations, and also to evaluate what information should be collected for use in the litigation. The preservation obligation is ongoing and will continue until the litigation is fully resolved.

Pursuant to the discussion above about the duties of outside counsel, we ask that you please confirm in writing that you have received and understand the advice set forth above.

Thank you.

NOTICE TO PRESERVE EVIDENCE
READ IMMEDIATELY

TO: [Employees who may have relevant information]

FROM: [Attorney]

DATE: [Should be sent as soon as possible – see legal standard]

RE: Preservation of Documents for Litigation
[Case Name / Matter Description]

[Client X] is involved in a dispute concerning [describe matter, including the relevant facts, individuals and entities involved, time period at issue, and potential (or actual) claims].

[Client X] will likely need to review and produce information potentially relevant to these issues. To ensure that review and production is possible, [client X] is obligated to take affirmative steps immediately to preserve documents (both paper documents and electronically stored information ("ESI")) and any other evidence that is or may become relevant to this dispute, and that is within [client X's] possession, custody, or control ("Relevant Information"). This obligation extends to [client X's] officers, directors, employees, consultants, counsel, and accountants, among others. You have received this notice because you may have, or know of, Relevant Information.

The failure to preserve Relevant Information, including by deleting or altering electronically stored information, even if unintentional, could subject [client X] to a variety of sanctions, including monetary sanctions, legal rulings adverse to [client X's] position in this dispute, or entry of judgment against [client X].

A. Relevant Information that [Client X] Is Obligated to Preserve

[Client X] is obligated to preserve Relevant information as it exists in any media, including paper documents, electronically stored information, and tangible objects (machinery, models/mock-ups, etc.).

Paper documents include, among other things, letters, faxes, memoranda, notes, desk files, forms, spreadsheets, charts, calendar books, address books, agreements, telephone logs, and print-outs of electronically stored documents.

Electronically stored information may exist in a variety of forms and locations. Sources of potentially relevant electronically stored information that you should take steps to preserve include, but are not limited to, emails (regardless of whether they reside in an inbox, sent items folder, deleted items folder, or other location), electronic

document files (such as PDFs and Microsoft Word, Excel, and PowerPoint files), databases, audio/video files, image files, voicemail, text messages, instant messages, calendar entries, internet browser history, and online postings and other data stored on social networking sites (such as LinkedIn, Facebook, and Twitter).

This data may reside on network servers, personal computers, portable storage media (such as hard drives, thumb drives, flash drives, and optical discs), tablets, smartphones, backup tapes and disaster recovery systems, third-party internet sites, or cloud-based storage systems.

The preservation obligation extends to data on any devices, computers, email and online accounts, and other storage media that you own or control *personally*, in addition to any sources owned or controlled by [client X]. You should not distinguish between "official" firm files and "personal" or other "nonofficial" files for purposes of preserving Relevant Information.

This preservation obligation should be construed broadly and extends to drafts and duplicates of relevant documents. If there is any doubt about whether you should preserve a particular category or source of Relevant Information, you should err on the side of caution and do so.

B. What You Must Do

Please take the following steps immediately to ensure that Relevant Information is preserved:

1. Do not destroy, erase, delete, overwrite, or alter any Relevant Information. Do not open any electronic files that you believe may be subject to this hold – opening the document changes the "metadata" of the document.

2. Cease any process, practice, or procedure that might result in the destruction, erasure, deletion, or alteration of any Relevant Information.

3. Preserve any hardware and software that contains or is necessary to access any Relevant Information.

4. Preserve any passwords, decryption procedures (and accompanying software), network access codes, ID names, manuals, tutorials, written instructions, and decompression or reconstruction software.

[Provide any matter-specific details concerning documents to be preserved]

C. Duration of Litigation Hold

This preservation obligation will continue until further notice from [client X's representative or attorney]. You should preserve all Relevant Information now and continue to preserve Relevant Information in the future until you are directed to cease doing so. If you expect that any of these preservation steps will impose a significant

hardship (including because of the inability to access electronic files), please let [insert name] know immediately, and we will work to reduce the burden.

We will contact you when it becomes necessary to collect some or all of the Relevant Information that you are preserving.

Please acknowledge receipt of this notice and your agreement to abide by these procedures by signing and dating the acknowledgment below and returning it to [insert name]. Any questions regarding this notice should be directed to [insert name].

***

ACKNOWLEDGEMENT

I acknowledge receipt of the above Notice to Preserve Evidence and agree to abide by the procedures set forth therein.

By: _____

Title: _____

Date: _____

Preservation Demand Letter – Send to Opposing Counsel

[Date]

****
NOTICE TO PRESERVE EVIDENCE
****

BY CERTIFIED MAIL
RETURN RECEIPT REQUESTED

[Addressee
_____
_____
_____]

Subject: [Caption of Lawsuit]

Dear _____:

[Client] hereby notifies [opposing party] that [it/he/she/they] [is/are] obligated to preserve all documents, tangible things, and electronically stored information ("ESI") that may be relevant to the issues in the above-captioned action. This obligation extends to any documents within the possession, custody, or control of [opposing party], along with [opposing party's] predecessors, successors, parents, subsidiaries, divisions, affiliates, and third-party service providers, and their respective officers, directors, agents, attorneys, accountants, employees, partners or other persons occupying similar positions or performing similar functions.

At the appropriate time, we intend to seek information related to [describe] through discovery. Failure to preserve relevant documents may result in severe penalties, including monetary sanctions, adverse jury instructions, or even entry of judgment against [opposing party].

At a minimum, the following information may be relevant to this matter and should be preserved:

[Describe]

Please take immediate steps to preserve potentially relevant documents, tangible things, or ESI in their current form, without any alterations, including by preserving any drafts and document metadata. The rules prohibiting destruction of evidence apply to ESI in the same manner that they apply to other evidence. Due to its format, electronic information is easily deleted, modified, or corrupted. Accordingly, please also cease any process, practice, or procedure, such as automated deletion of ESI and recycling of backup tapes that may result in the destruction, erasure, deletion, alteration, or overwriting of any relevant or potentially relevant ESI.

For purposes of preservation, ESI should be afforded the broadest possible meaning and should include any information stored in any electronic medium, including, without limitation, network servers, personal computers, portable storage media (such as hard drives, thumb drives, flash drives, and optical discs), tablets, smartphones, backup tapes and disaster recovery systems, third-party internet sites, or cloud-based storage systems. ESI includes the following categories of data (by way of example only and not as an exclusive list): emails, voicemails, instant messages (e.g., SMS, iMessage, BBM files), word processing files (e.g., Microsoft Word files), spreadsheets and tables (e.g., Microsoft Excel files), presentations (e.g., Microsoft PowerPoint files), PDF files, image files (e.g., .TIFF, .JPG, .GIF, .BMP files), audio files (e.g., .WAV, .MP3 files), video files (e.g., .AVI, .MOV files), databases, calendar entries, contact and relationship management data, network access and server activity logs, online access data (e.g., browser history, temporary internet files, cookies), online postings and other data stored on social networking sites (e.g., LinkedIn, Facebook, Twitter), and backup and archival files (e.g., .ZIP, .GHO, .RAR files).

In addition to preserving relevant ESI, you should also preserve any hardware or software that contains, or is necessary to access, any potentially relevant data. Please also preserve any passwords, decryption procedures (and accompanying software), network access codes, ID names, manuals, tutorials, written instructions, and decompression or reconstruction software.

Please forward a copy of this letter to all persons or entities with custodial responsibility for the items referred to in this letter.

If this correspondence is in any way unclear, or if you would like to discuss [opposing party]'s preservation obligations further, please contact us immediately.

Very truly yours,

[ATTORNEY]

STIPULATION AND ORDER RE: USE OF PREDICTIVE CODING IN DISCOVERY

WHEREAS, Plaintiff _____ and Defendant _____ (collectively the "Parties" and each a "Party") in the above-captioned litigation ("Action") agree to the use of predictive coding for the search, review, and production of documents in this Action and to enter a stipulation ("Stipulation") to memorialize their agreement;

IT IS HEREBY STIPULATED AND AGREED, by and between the undersigned, as attorneys of record for the Parties, as follows:

1. Definitions

(a) "Precision" means the fraction of documents identified as likely responsive by the Predictive Coding Process that are in fact responsive.[1]

(b) "Predictive Coding Process" means the use of Predictive Coding Software to categorize documents into those that are likely responsive and those that are likely non-responsive.

(c) "Predictive Coding Software" means the software a Party elects to use to perform the Predictive Coding Process.

(d) "Recall" means the fraction of responsive documents that are identified as likely responsive by the Predictive Coding Process.

(e) "Statistically Valid Sample" means a random sample of sufficient size and composition to permit statistical extrapolation with a margin of error of +/2% at the 95% confidence level.[2]

2. Scope of this Stipulation

(a) The procedures described in this Stipulation govern the use of predictive coding to assist in the production of documents by the Parties to this Action. In this Stipulation, predictive coding shall mean and refer to a process for selecting and ranking a collection of documents using a computerized system that incorporates the decisions that lawyers have made on a smaller set of documents and then applying those decisions to the remaining universe of documents.

(b) Nothing in this Stipulation shall prevent the Party responding to discovery (the "Responding Party") from using other search, review, or coding methodologies in addition to, or in place of,

[1] Definitions of "Precision" and "Recall" are adapted from the "Grossman–Cormack Glossary of Technology–Assisted Review," 7 Fed. Cts. L.Rev. 1, 25, 27 (2013).

[2] The size of the sample will vary depending upon several factors, and shall be calculated using the formula $n = \frac{X^2 * N * P * (1-P)}{(ME^2 * (N-1)) - (X^2 * P * (1-P))}$, where, ME is the margin of error; X is the Confidence Level (1.96 for a 95% Confidence Level); P is judgment of richness, N is the population and n is sample size. Where richness is not reasonably estimable, 0.5 may be used. Based on a Confidence Level of 95%, richness of 0.5, a Population of 1,000,000, and a margin of error of 2%, the resulting sample size is 2,395 documents.

predictive coding to help identify documents that are responsive to the document requests from the Party seeking discovery (the "Requesting Party").

3. Initial Disclosure of Information about Predictive Coding

(a) Prior to the commencement of any review using predictive coding, the Responding Party shall disclose to the Requesting Party in writing its intention to use predictive coding and the following information:

(i) The name, publisher, version number, and a description of the Predictive Coding Software and Predictive Coding Process;

(ii) The name and qualifications of the person who will oversee the implementation of the predictive coding process (the "Technical Expert");

(iii) A description of the documents to be subjected to predictive coding (the "Document Universe"), including:

(1) Custodian/Source;

(2) Data types (e.g., email, electronic documents, etc.);

(3) The number of documents in the Document Universe, in total and for each Custodian/Source;

(iv) The responsiveness categories into which the Document Universe is to be categorized (the "Responsiveness Categories").

(b) The Parties shall meet and confer to address any questions or disputes about the selection of the Predictive Coding Software, the Technical Expert, the Document Universe, and the Responsiveness Categories, and the Responding Party shall make its Technical Expert reasonably available to address questions about the technical operation of the Predictive Coding Software.

4. Predictive Coding Methodology

(a) Culling the Document Universe. If the Responding Party determines it to be reasonable and appropriate, the Responding Party may use search terms and other criteria (the "Culling Criteria") to reduce the volume of the Document Universe. If it does so, the Responding Party shall promptly:

(i) Disclose in writing to the Requesting Party the Culling Criteria used and the number of documents removed by the Culling Criteria (the "Excluded Documents");

(ii) Review a Statistically Valid Sample from the Excluded Documents, disclose the size of that sample set, and produce any responsive, non-privileged documents the Responding Party identifies;

(iii) Meet and confer with the Requesting Party, if requested, to address any questions or disputes about the reasonableness and appropriateness of the Culling Criteria.

(b) Control Set Review. To aid in the Predictive Coding Process, and to determine the prevalence of responsive information from the Document Universe, the Responding Party shall review a Statistically Valid Sample of documents from the Document Universe (the "Control Set"). Prior to the commencement of Seed Set Identification, see 4(c) below, the Responding Party shall disclose the results of the review of the Control Set to the Requesting Party, including the number of documents in the Control Set and the number of documents that were coded for each of the Responsiveness Categories during the review of the Control Set. The Responding Party shall produce all non-privileged documents reviewed in the Control Set, and for each document disclose the Responsiveness Categories, if any, to which it is responsive. The Requesting Party shall raise any disputes regarding how the documents were coded for each of the Responsiveness Categories in the Control Set within five (5) business days of the production of 4,000 documents or fewer or ten (10) business days of the production of more than 4,000 documents. The parties agree to meet and confer in good faith over any such disputes. All non-responsive documents produced from the Control Set shall be deemed "Highly Confidential" under the terms of the Stipulated Protective Order (Dkt. No. __), shall be used only for the purpose of evaluating the accuracy of the document coding, and shall be promptly returned or destroyed after review by the Requesting Party and the resolution of any disputes.

(c) Seed Set Identification. The Responding Party may use any reasonable method, including, but not limited to, search terms, to identify a set of documents to be used to initially train the Predictive Coding Software (the "Seed Set"). Prior to commencement of Training, see 4(d) below, the Responding Party shall disclose to the Requesting Party in writing a description of the size of the Seed Set and the methodology used to identify it. The Responding Party shall produce all non-privileged documents and disclose for each document the Responsiveness Categories, if any, to which it is responsive. The Requesting Party shall raise any disputes regarding how the documents were coded within five (5) business days of the production of 4,000 documents or fewer or ten (10) business days of the production of more than 4,000 documents. The parties agree to meet and confer in good faith over any such disputes. All non-responsive documents produced from the Seed Set shall be deemed "Highly Confidential" under the terms of the Stipulated Protective Order (Dkt. No. __), shall be used only for the purpose of evaluating the accuracy of the document coding, and shall be promptly returned or destroyed after review by the Requesting Party and the resolution of any disputes.

(d) Training Sets. The Responding Party may use any reasonable method to train the Predictive Coding Software. Upon completion of the training, the Responding Party shall disclose in writing the results of the training to the Requesting Party, including, to the extent reasonably available, the number of documents reviewed, the number of documents coded for each of the Responsiveness Categories during training, the number of documents identified as likely responsive by the Predictive Coding Process, and the estimated rates of Recall and Precision

with their associated error margins. The Responding Party shall produce all non-privileged documents used to train the Predictive Coding Software and disclose for each document the Responsiveness Categories, if any, to which it is responsive. The Requesting Party shall raise any disputes regarding how the documents were coded within ten (10) business days of their production, and the parties agree to meet and confer in good faith over any such disputes. All non-responsive documents produced shall be deemed "Highly Confidential" under the terms of the Stipulated Protective Order (Dkt. No. __), shall be used only for the purpose of evaluating the accuracy of the document coding, and shall be promptly returned or destroyed after review by the Requesting Party and the resolution of any disputes.

(e) Uncategorized Documents. The Responding Party shall disclose the number of documents the Predictive Coding Software is unable to evaluate for any reason, including the unavailability of machine-readable text or documents that could not be ranked, and review such documents in their entirety in order to identify responsive, non-privileged documents for production.

(f) Validation Set. Prior to production, the Responding Party shall review a Statistically Valid Sample of documents in the Document Universe that are categorized as likely non-responsive by the Predictive Coding Process (the "Purported Non–Responsive Documents") in order to determine the prevalence of responsive documents that are contained therein. Prior to production, the Responding Party shall disclose to the Requesting Party in writing the number of Purported Non–Responsive Documents, the size of the Validation Set, the number of documents identified as responsive during the review of the Validation Set, and the implied rate of Recall. The Responding Party shall produce any responsive, non-privileged documents it identifies during the review of the Validation Set.

5. General Provisions.

(a) The Parties hereby agree to meet and confer in good faith over any disputes that might arise with respect to the terms and conditions of this Stipulation or any other aspects relating to discovery. The Responding Party agrees to make its Technical Expert reasonably available to the Requesting Party for questions about its use of predictive coding. Should the Parties be unable to resolve their disputes on any issues stemming from the use of predictive coding set forth in this Stipulation, they shall submit those issues to the Court for resolution.

(b) Notwithstanding the provisions set forth in this Stipulation, the Parties respectively reserve their rights regarding the instant discovery process. This includes, but is not limited to, the Requesting Party's right to object to the efforts of the Responding Party to search for, review, and produce information in response to the Requesting Party's document requests; and the Responding Party's right to withhold information pursuant to the objections it previously interposed in response to the Requesting Party's document requests.

Requests for Production - Sample Instructions for Form of ESI

Native Production:

Electronically stored information (ESI) must be produced in native format (the file format in which they are ordinarily maintained in the usual course of business) or in a format as close to native as practicable (e.g., .PST or .NSF format for e-mail messages, .DOC or .DOCX for Word documents, .XLS or .XLSX for Excel spreadsheets, .PPT or .PPTX for PowerPoint presentations, .MDB and . ACCDB for Microsoft Access databases, .WPD for WordPerfect documents, .PDF for Adobe Acrobat documents, .JPG, .JPEG, and .PNG for images). Whenever possible, ESI must be produced within the folders and subfolders in which it is kept in the usual course of business.

TIFF/Native Production:

Electronically stored information (ESI) must be converted to standard Group IV single-page TIFF files and produced with OCR text extraction files and a Concordance load file. ESI that cannot be converted into TIFF format without losing information or functionality (e.g., Excel files, PowerPoint files, databases, CAD Files, video files, audio files, and documents containing electronic comments or track changes) must be produced in native format (the file format in which the files are ordinarily maintained in the usual course of business). The Concordance load file must include links to any native files and metadata for all documents, including but not limited to the following fields as appropriate for the file type: author(s), recipient(s), carbon copy recipient(s), blind copy recipient(s), subject, file name, document type, custodian, date sent, time sent, file creation date, file modification date, access date, last saved by, file path, and folder information. E-mails must be produced preserving the local time. [Plaintiff/Defendant] reserves the right to request native files of any documents that are unreadable or have limited accessibility in TIFF format.

ESI Topics to Consider Discussing/Be Prepared to Discuss During the Rule 26(f) Discovery Conference[1]

1. Preservation
    a. What data sources are being preserved? What custodian accounts are being preserved? [2]
    b. When was the hold issued?
    c. How is compliance being monitored?
    d. Have automated deletion and janitorial functions been disabled?
    e. Have data sources with ephemeral or transitory data, such as smartphones, social media and other website data, and third-party hosted data, been collected for preservation?
    f. How will data be preserved when an employee leaves the company or transfers to a different position?
    g. Do all categories of documents that are currently preserved need to be preserved going forward? Can the preservation obligation be limited as new data is created?
2. Scope of Discovery
    a. What is the relevant data that will most likely need to be collected and reviewed?
    b. Who are the custodians likely to possess relevant data?
    c. What technical obstacles exist regarding the collection of documents?
    d. What third-party discovery is necessary?

[1] Consult all applicable civil rules, and any specific requirements set out in standing orders or case management orders issued by the court, before the conference. Some judges have particular requirements for what they expect the parties to have discussed prior to the Rule 16 conference that generally follows the Rule 26f conference.
[2] Which custodians may have relevant data and therefore are subject to the litigation hold may be information protected by attorney work-product. Other pieces of information relating to preservation may also be subject to attorney-client privilege or work-product protection. If a decision is made to refuse to disclose this kind of information, be prepared to explain why the information is protected from disclosure.

3. Collection, Filtering, and Review
    a. What filtering methodologies will be used? (E.g., keyword searching, de-duplication, date limitations)
    b. Who will conduct the review? Are there any obstacles to use of outside reviewers, such as foreign data protection issues, or confidentiality issues?
    c. Is either party considering using alternative methods of review, such as predictive coding?
4. Production
    a. In what form will documents be produced? (E.g., TIFFs, native files, mix)
    b. Are all parties agreeable to standard load file specifications (e.g. extracted metadata)?
    c. How will data from nonstandard sources (e.g., websites and mobile devices) be produced?
    d. Will the parties agree to permit rolling productions?
    e. Is any party going to insist that documents be coded to correspond to specific document requests?
5. Privilege Issues
    a. Will the parties consent to a clawback agreement or other similar stipulation? Is it necessary that the agreement be entered as a court order?
    b. How should the parties log documents withheld on privilege grounds?
        i. What form should the log take?
        ii. What information must be included?
        iii. Do the logs need to list email attachments and down-chain emails separately?

iv. What are the parties' views with respect to nontraditional privilege logs, such as logs that list documents by category instead of individual record?

v. When will the logs be produced?

vi. What protocol should be used to request additional information about a log entry or challenge a privilege determination?

6. Other Means of Reducing Costs

    a. Could phased discovery be used to reduce costs?

    b. Could a FRE 502 clawback agreement be used to reduce cost of review for privilege?

IN THE UNITED STATES DISTRICT COURT
FOR [INSERT]

[insert], Plaintiff	§	
vs.	§	NO. [insert]
[insert], Defendants.	§	STIPULATED PROTECTIVE ORDER

Unless this order includes a clause that explicitly states that a particular local civil rule is modified as applied to this case, nothing in this order shall be construed to modify the provisions, operation, or effect of any local civil rule of this court. Notwithstanding any other clause to the contrary, this order cannot be modified except by court order.

The parties must not unreasonably file under seal pleadings, motions, or other papers that do not qualify under this protective order for filing under seal. The parties must attempt to file unsealed as much of a pleading, motion, or other paper as they reasonably can without undermining the protections conferred by this protective order

1. PURPOSES AND LIMITATIONS

Discovery requests filed in this action call for the production of certain confidential information within the meaning of Fed. R. Civ. P. 26(c) or other private or sensitive information for which special protection from public disclosure and from use for any purpose other than prosecuting this litigation is warranted. Accordingly, the parties hereby stipulate to and petition the Court to enter the following Stipulated Protective Order pursuant to Fed. R. Civ. P. 26(c).

2. DEFINITIONS

2.1 Party. Any party to this action, including all of its officers, directors, and principals.

2.2 Discovery Material. All items or information, regardless of the medium or manner generated, stored, or maintained (including, among other things, documents, testimony,

transcripts, tangible things, or discovery responses) that are produced or generated in connection with discovery in this matter.

2.3 Confidential Information or Items. All items or information, regardless of the medium or manner generated, stored, or maintained, that has been designated as "Confidential" or "Confidential—Attorney's Eyes Only."

2.4 Producing Party. Any Party or non-party that produces Discovery Material in this action.

2.5 Receiving Party. Any Party or non-party that receives Discovery Material from a Producing Party.

2.6 Designating Party. Any Party or non-party that designates Discovery Material as "Confidential" or "Confidential—Attorney's Eyes Only."

2.7 Protected Material. Any Discovery Material that is designated as "Confidential" or "Confidential—Attorney's Eyes Only."

2.8 Outside Counsel. Attorneys, along with their paralegals, and other support personnel, who are not employees of a Party but who are retained to represent or advise a Party in this action.

2.9 In House Legal Personnel. Attorneys and other personnel employed by a Party to perform legal functions who are responsible for overseeing this litigation for the Party.

2.10 Counsel (without qualifier). Outside Counsel and In House Legal Personnel (as well as their support staffs, including but not limited to attorneys, paralegals, secretaries, and law clerks.).

2.11 Expert, Consultant and/or Investigator. A person with specialized knowledge or experience in a matter pertinent to the litigation, along with his or her employees and support personnel, who has been retained by a Party or its Counsel to serve as an expert witness, consultant or as an investigator in this action, and who is not currently an employee, nor has been an employee within four years of the date of entry of this Order, of a Party and who, at the time of

retention, is not anticipated to become an employee of a Party. This definition includes a professional jury or trial consultant retained in connection with this litigation.

2.12 Professional Vendors. Persons or entities that provide litigation support services (e.g. , photocopying; videotaping; translating; preparing exhibits or demonstrations; organizing, storing, or processing data in any form or medium; etc.) and their employees and subcontractors.

3. SCOPE

The protections conferred by this Order cover not only Protected Material (as defined above), but also any information copied or extracted therefrom, as well as all copies, excerpts, summaries, or compilations thereof, plus testimony, conversations, or presentations by Parties or Counsel in settings that might reveal Protected Material. However, this Order shall not be construed to cause any Counsel to produce, return, and/or destroy their own attorney work product, or the work product of their co-counsel.

4. DURATION

The confidentiality obligations imposed by this Order shall remain in effect until the Designating Party agrees otherwise in writing or this Court orders otherwise.

5. DESIGNATING PROTECTED MATERIAL

5.1 Exercise of Restraint and Care in Designating Material for Protection. The designation by any Designating Party of any Discovery Material as "Confidential" or "Confidential—Attorney's Eyes Only" shall constitute a representation that such Discovery Material has been reviewed by an attorney for the Designating Party and that there is a good faith basis for such designation.

5.2 Manner and Timing of Designations. Except as otherwise provided in this Order (see, e.g., Sections 5.2(b) and 5.4), or as otherwise stipulated or ordered, material that qualifies for protection under this Order must be clearly so designated before the material is disclosed or produced.

Designation in conformity with this Order requires:

(a) for information in documentary form (including transcripts of depositions taken in other proceedings), that the Producing Party affix the legend "CONFIDENTIAL" or "CONFIDENTIAL—ATTORNEY'S EYES ONLY" on each page that contains protected material.

(b) for deposition transcripts and/or exhibits, that the Designating Party designate any portion of the testimony as "CONFIDENTIAL" or "CONFIDENTIAL—ATTORNEY'S EYES ONLY" either on the record before the deposition is concluded, or in writing on or before the later of (i) fourteen (14) days after the final transcript is received or (ii) the date by which any review by the witness and corrections to the transcript are to be completed under Fed. R. Civ. P. 30(e). Only those portions of the testimony that are designated for protection in accordance with the preceding sentence shall be covered by the provisions of this Order. The entire testimony shall be deemed to have been designated "CONFIDENTIAL—ATTORNEY'S EYES ONLY" until the time within which the transcript may be designated has elapsed. If testimony is not designated within the prescribed time period, then such testimony shall not be deemed "CONFIDENTIAL" or "CONFIDENTIAL—ATTORNEY'S EYES ONLY" except as ordered by the Court.

Transcript pages containing Protected Material must be separately bound by the court reporter, who must affix to each such page the legend "CONFIDENTIAL" or "CONFIDENTIAL—ATTORNEY'S EYES ONLY" as instructed by the Designating Party.

(c) for information produced in electronic, audio, or video format, and for any other tangible items, that the Producing Party affix in a prominent place on the exterior of the container or containers in which the information or item is stored the legend "CONFIDENTIAL" or "CONFIDENTIAL—ATTORNEY'S EYES ONLY. "

5.3 Inadvertent Failures to Designate. Should a Producing Party discover that it produced material that should have been but was not designated as Protected Material, the Producing Party shall notify all Parties, identifying (by bates number or other individually

identifiable information) the affected documents and their new designation or re-designation. Thereafter, the material so designated or re-designated will be treated as Protected Material. Promptly after providing such notice, the Producing Party shall provide re-labeled copies of the material to each Receiving Party reflecting the change in designation. The Receiving Party shall make reasonable efforts to return or destroy the incorrectly designated material. If corrected, a failure to designate qualified information or items as "CONFIDENTIAL" or "CONFIDENTIAL—ATTORNEY'S EYES ONLY" does not, standing alone, waive the Producing Party's right to secure protection under this Order for such material. If material is re-designated as "CONFIDENTIAL" or "CONFIDENTIAL—ATTORNEY'S EYES ONLY" after the material was initially produced, the Receiving Party, upon notification of the designation, must make reasonable efforts to assure that the material is treated in accordance with the provisions of this Order.

6. CHALLENGING CONFIDENTIALITY DESIGNATIONS

6.1 Meet and Confer. A Party that elects to initiate a challenge to a Designating Party's confidentiality designation must do so in good faith and must begin the process by notifying the Designating Party in writing, by telephone or in person of its challenge and identifying the challenged material, then conferring directly with counsel for the Designating Party. Each Party must explain the basis for its respective position about the propriety of the challenged confidentiality designations.

6.2 Judicial Intervention. In any judicial proceeding challenging a confidentiality designation, the burden of persuasion with respect to the propriety of the confidentiality designation shall remain upon the Designating Party. If the Parties are not able to resolve a dispute about a confidentiality designation within the time provided in Section 6.2, above, the Receiving Party who challenges the designation shall, within 14 days thereafter, make a motion to the Court under this Court's local motion rules. Until the Court rules on the dispute, all Parties

shall continue to treat the material in question as "CONFIDENTIAL" or "CONFIDENTIAL—ATTORNEY'S EYES ONLY."

In the event that the final ruling is that the challenged material is not "CONFIDENTIAL" or "CONFIDENTIAL—ATTORNEY'S EYES ONLY," the Designating Party shall reproduce copies of all materials with their designations removed in accordance with the ruling within thirty (30) days at the expense of the Designating Party.

7. ACCESS TO AND USE OF PROTECTED MATERIAL

7.1 Basic Principles. A Receiving Party may use Protected Material that is disclosed or produced by a Producing Party only in connection with this action for prosecuting, defending, or attempting to settle this action; appealing from any order or judgment entered in this action; or obtaining insurance coverage or indemnification relating to this action. Protected Material may not be used for any other purpose, including, without limitation, any business or commercial purpose, or for the purposes of any other litigation, action, or legal or regulatory proceeding. Protected Material may be disclosed only to the categories of persons and under the conditions described in this Order. When the litigation has been terminated, a Receiving Party must comply with the provisions of Section 11, below (FINAL DISPOSITION).

7.2 Disclosure of Confidential Information or Items. Unless otherwise ordered by the Court or permitted in writing by the Designating Party, a Receiving Party may disclose any information or item designated "CONFIDENTIAL" only to:

(a) the Receiving Party's Counsel;

(b) Counsel to any other Parties to this action;

(c) the Parties and, to the extent any Party is not a natural person, officers, directors and principals of such a Party to whom disclosure is reasonably necessary for this litigation;

(d) former officers, directors, or principals, and current or former employees of corporate Parties to whom disclosure is reasonably necessary for this litigation and who have signed the "Agreement To Be Bound By Protective Order" (Exhibit A);

(e) Experts and/or Consultants to whom disclosure is reasonably necessary for this litigation and who have signed the "Agreement To Be Bound By Protective Order" (Exhibit A);

(f) the Court and its personnel;

(g) court reporters and/or videographers, their staffs, and Professional Vendors to whom disclosure is reasonably necessary for this litigation and who have signed the "Agreement To Be Bound By Protective Order" (Exhibit A);

(h) the author, addressees, or recipients of the document;

(i) any other natural person who would have likely reviewed such document during his or her employment as a result of the substantive nature of his or her employment position, or who is specifically identified in the document, or whose conduct is purported to be specifically identified in the document and who have signed the "Agreement To Be Bound By Protective Order" (Exhibit A);

(j) deponents or witnesses in the action, and their Counsel, to whom disclosure is reasonably necessary for this litigation and who have signed the "Agreement To Be Bound By Protective Order" (Exhibit A); and

(k) any other person to whom the Designating Party agrees in writing or on the record, and any other person to whom the Court compels access to the Confidential Information or Items.

7.3 Disclosure of "CONFIDENTIAL—ATTORNEY'S EYES ONLY" Information or Items. Unless otherwise ordered by the Court or permitted in writing by the Designating Party, a Receiving Party may disclose any information or item designated "CONFIDENTIAL—ATTORNEY'S EYES ONLY" only to:

(a) the Receiving Party's Counsel;

(b) Counsel to any other Parties to this action;

(c) Experts and/or Consultants to whom disclosure is reasonably necessary for this litigation and who have signed the "Agreement To Be Bound By Protective Order" (Exhibit A);

(d) the Court and its personnel;

(e) court reporters and/or videographers, their staffs, and Professional Vendors to whom disclosure is reasonably necessary for this litigation and who have signed the "Agreement To Be Bound By Protective Order" (Exhibit A);

(f) the author, addressees, or recipients of the document;

(g) any other person to whom the Designating Party agrees in writing or on the record, and any other person to whom the Court compels access to the "CONFIDENTIAL—ATTORNEY'S EYES ONLY" Information or Items.

7.4 Retention of Exhibit A. Outside Counsel for the Party that obtains the signed "Agreements To Be Bound By Protective Order" (Exhibit A), as required above, shall retain them for one year following the final termination of this action, including any appeals, and shall make them available to other Parties upon good cause shown.

7.5 Retention of Protected Material. Persons who have been shown Protected Material pursuant to Section 7.2(c), (d), (e), (i), (j) or (k) or Section 7.3(c) or (g) shall not retain copies of such Protected Material.

8. PROTECTED MATERIAL SUBPOENAED OR ORDERED PRODUCED IN OTHER LITIGATION

If a Receiving Party is served with a discovery request, subpoena or an order issued in other litigation that would compel disclosure of any information or items designated in this action as "CONFIDENTIAL" or "CONFIDENTIAL—ATTORNEY'S EYES ONLY, " the Receiving Party must notify the Designating Party, in writing (by fax or electronic mail, if possible), along with a copy of the discovery request, subpoena or order, as soon as reasonably practicable.

The Receiving Party also must promptly inform the party who caused the discovery request, subpoena or order to issue in the other litigation that some or all of the material covered by the subpoena or order is the subject of this Order. In addition, the Receiving Party must deliver a copy of this Order promptly to the party in the other action that caused the discovery request, subpoena or order to issue. The Receiving Party shall not produce the requested Protected Material unless and until the court so directs, except if the Designating Party (a) consents, or (b) fails to file a motion to quash or otherwise contest the production of the Protected Material prior to the date designated for production of the Protected Material, in which event the Receiving Party may produce on the production date, but no earlier.

The purpose of imposing these duties is to alert the interested parties to the existence of this Order and to afford the Designating Party in this action an opportunity to try to protect its confidentiality interest in the court from which the discovery request, subpoena or order is issued. The Designating Party shall bear the burdens and the expenses of seeking protection in that court of its Protected Material. Nothing in these provisions should be construed as authorizing or encouraging a Receiving Party in this action to disobey a lawful directive from another court or regulatory agency.

9. UNAUTHORIZED DISCLOSURE OF PROTECTED MATERIAL

If a Receiving Party learns that, by inadvertence or otherwise, it has disclosed Protected Material to any person or in any circumstance not authorized under this Order, the Receiving Party must promptly (a) notify in writing the Designating Party of the unauthorized disclosures, (b) use its best efforts to retrieve all copies of the Protected Material, (c) inform the person or persons to whom unauthorized disclosures were made of all the terms of this Order, and (d) request such person or persons to execute the "Agreement To Be Bound by Protective Order" (Exhibit A).

10. FILING PROTECTED MATERIAL

Unless otherwise ordered by the Court or agreed to in writing by the Parties, any documents filed with the Court, including but not limited to pleadings, memoranda, transcripts,

and discovery responses, which contain or refer to any Protected Material, shall be filed under seal or with redactions, as appropriate. Each such filing shall be made electronically in accordance with this Court's guidelines on "Electronic Case Filing: Filing a Sealed and/or Ex Parte Document in a Civil Case" and Local Rule 79.3. The word "Sealed" shall be used in the title or caption of both the motion and any proposed order. It is the responsibility of the Designating Party to comply with Local Rule 79.4 if it wishes any Protected Material to remain under seal following final disposition of this case.

11. FINAL DISPOSITION

Unless otherwise ordered or agreed in writing by the Producing Party, within sixty (60) days after the final termination of this action, including any appeals, each Receiving Party must make reasonable efforts to return or destroy all Protected Material to the Producing Party. As used in this section, "Protected Material"includes all copies, abstracts, compilations, summaries or any other form of reproducing or capturing any of the Protected Material. Whether the Protected Material is returned or destroyed, the Receiving Party must submit a written certification to the Producing Party (and, if not the same person or entity, to the Designating Party) by the sixty-day deadline that it has complied with the terms of this provision. Notwithstanding this provision, Counsel are entitled to retain an archival copy of all pleadings, motion papers, transcripts, legal memoranda, correspondence or attorney work product, even if such materials contain Protected Material. Any such archival copies that contain or constitute Protected Material remain subject to this Order as set forth in Section 4 (DURATION), above.

12. INADVERTENTLY PRODUCED DOCUMENTS

Pursuant to Fed. R. Evid. 502, if a Party at any time notifies any other Party that it inadvertently disclosed documents, testimony, information, and/or things that are protected from disclosure under the attorney-client privilege, work product doctrine, and/or any other applicable privilege or immunity from disclosure, or the Receiving Party discovers such inadvertent

disclosure, the inadvertent disclosure shall not be deemed a waiver of the applicable privilege or protection.

Except as provided in the last sentence of this paragraph, the Receiving Party shall immediately return or destroy all copies of such documents, testimony, information and/or things to the inadvertently disclosing Party, shall provide a certification of counsel that all inadvertently disclosed materials have been returned or destroyed, and shall not use such items for any purpose until further order of the Court. In all events, such return or destruction and certification must occur within five (5) business days of receipt of notice or discovery of the inadvertent disclosure. Within five (5) business days of the notification that the inadvertently disclosed materials have been returned or destroyed, the inadvertently disclosing Party shall produce a privilege log with respect to the inadvertently disclosed materials. The return of any Discovery Material to the inadvertently disclosing Party shall not in any way preclude the Receiving Party from moving the Court for a ruling that the disclosed information was never privileged and, for that purpose, may submit a copy of such materials to the Court for in camera review in connection with any such motion.

13. ATTORNEY RENDERING ADVICE

Nothing in this Order will bar or otherwise restrict an attorney from rendering advice to his or her client with respect to this matter or from relying upon or generally referring to Protected Material in rendering such advice; provided however, that in rendering such advice or in otherwise communicating with his or her client, the attorney shall not reveal or disclose the specific content thereof if such disclosure is not otherwise permitted under this Order.

14. TRIAL

The terms of this Order shall govern in all circumstances except for presentations of evidence and argument at trial. The parties shall meet and confer in advance of such proceedings and seek the guidance of the Court as to appropriate procedures to govern such proceedings.

15. MISCELLANEOUS

15.1 Right to Further Relief. Nothing in this Order abridges the right of any person to seek its modification by the Court in the future.

15.2 Right to Assert Other Objections. By stipulating to the entry of this Order no Party waives any right it otherwise would have to object to disclosing or producing any information or item on any ground not addressed in this Order. Similarly, no Party waives any right to object on any ground to use in evidence of any of the material covered by this Order.

IT IS SO STIPULATED, THROUGH COUNSEL OR RECORD.

Dated:

Respectfully submitted,

[add signature block]

[add signature block]

The Court having found that good cause exists for issuance of an appropriately-tailored protective order pursuant to Fed. R. Civ. P. 26(c), it is therefore hereby

SO ORDERED.

[date]

UNITED STATES DISTRICT JUDGE

Exhibit A to Stipulated Protective Order

AGREEMENT TO BE BOUND BY PROTECTIVE ORDER

I,_____[print full name], under penalty of perjury under the laws of the United States of America state as follows.

My residence address is: _____

My current employer is: _____

My business address is: _____

My business telephone is: _____

I have read and understand in its entirety the Stipulated Protective Order that was issued by the United States District Court for [insert], in the case of [insert], dated [insert].

I agree to comply with and to be bound by all the terms of this Stipulated Protective Order, and I understand and acknowledge that failure to so comply could expose me to sanctions and punishment in the nature of contempt of court, money damages, interim or final injunctive relief and/or such other relief that the Court deems appropriate. I solemnly promise that I will not disclose in any manner any information or item that is subject to this Stipulated Protective Order to any person or entity except in strict compliance with its provisions.

I further agree to submit to the jurisdiction of the United States District Court for [insert] solely for the purpose of enforcing the terms of this Stipulated Protective Order, even if such enforcement proceedings occur after termination of this action.

Date: _____

City and State (or Country) where sworn and signed: _____

Printed name: _____

Signature: _____

Issues List for Deposition of a Corporate Representative Regarding ESI

(Use for Preparing Deponent And Preparing to Take Deposition)

1. Is the witness competent to testify?[1]
    a. Consider the ESI-related topics set forth in the deposition notice carefully. Ensure that the selected witness is competent, or can be educated, to testify about all of them.
    b. Understand the witness's background and experience with respect to technology issues.
    c. Understand the witness's role at the company and with respect to electronic discovery in the litigation.
2. Technology Infrastructure - Understand details regarding the following:
    a. The company's email and instant messaging systems
    b. The company's voicemail system
    c. The company's computer and server systems, including the number, types, and locations of computers in use and no longer in use
    d. The company's operating systems and application software
    e. The company's file-naming and location-saving conventions
    f. The company's use of cloud-based storage including policies on use – only educate on actual practices if within scope of deposition
    g. The company's policies on, and support of, employees use of mobile devices for work purposes
    h. The company's backup, archival, and disaster recovery systems and schedules
    i. Locations likely to contain ESI relevant to the subject matter of the case

[1] Failure to produce a competent witness can subject a party to sanctions under Fed. R. Civ. P. 37(d).

j. Digital records management policies and procedures
k. Corporate policies regarding employee use of company computers and employee use of personal computers and devices for company business
l. Details regarding employee access to network administration, backup, archiving, or other system operations during the relevant period
m. Details regarding any changes to technology at the company during the relevant period

3. Document Preservation
    a. When was a litigation hold implemented?
    b. How was the hold implemented?
        i. What custodians, systems, servers, computers, and devices were subject to the hold?
        ii. Which automated deletion and janitorial systems were disabled with respect to sources that may contain relevant data?
    c. What has been done to verify compliance with the hold?
4. Document Collection & Review
    a. What process was used to collect relevant documents?
        i. From which custodians did the company collect ESI?
        ii. What search terms were used?
        iii. What date range limiters were used?
    b. How was the review conducted?

Sample Deposition Topics/Questions on E-Discovery Issues

Note: Many of these questions are only appropriate for a 30(b)(6)-type deposition of a records manager or IT supervisor. *See* Issues List for Corporate Deponent. However, many topics can be used with an individual. As with all guidance on this page, these are suggestions only.

Persons Responsible

1) Tell me which people employed by *respondent* who are responsible for the maintenance, creation, modification or implementation of *respondent's* information technology system (including but not limited to *RESPONDENT'S* network, archival system, computers and storage devices)

2) Tell me which people employed by *respondent* are responsible for creating or modifying any policies or procedures related to the information technology system

3) Tell me what consultants or outside vendors *respondent* uses for maintenance and service of information technology systems (including but not limited to *respondent's* network, archival system, computers and storage devices)

4) Tell me what outside vendors *respondent* uses for any outsourced information storage or management, such as cloud-based storage vendors

5) Tell me which of *respondent's* personnel are responsible for managing relationships with any vendors that have a role in *respondent's* information technology systems.

Respondent's Systems

6) I'd like for you to describe for me the architecture of *respondent's* information technology system, including the following particulars:

a) Tell me the number and type of storage devices including, but not limited to, the storage devices used by users in the *[business unit]* used at the user level at present, and also during the relevant time period;

b) Tell me about any non-device storage used by *respondent* including cloud services like Amazon Web Service, Dropbox, Google Docs, etc. [Drill down into: account holders; encryption; size limitations, etc.]

c) Tell me the type(s) of software used presently and during the relevant time period at the user level including, but not limited to, the software used by users in the *[business unit]*), including operating systems and application programs. [Drill down into: brand names and versions of software

programs, including but not limited to those used for electronic mail, voice mail, calendars, project management, word processing, and database management].

d) I'd now like you to describe *respondent's* network and archival system, including, but not limited to,

- the brands and versions of network and archival system software used during the relevant time period and presently,
- the operating system brand and version on which network and archival system software was running during the relevant time period and presently, and
- the hardware used by *respondent's* network and archival systems.

7) How is encryption used on storage devices (including, but not limited to, desktop and/or laptop computers) and for ESI (including, but not limited to, electronic communications such as e-mail and voice mail).

8) Describe for me *respondent's* policy and/or standards pertaining to the use of *respondent's* storage devices away from the place of work for business purposes.

9) Describe for me *respondent's* policy pertaining to the use of *respondent's* storage devices for non-business purposes.

10) Describe for me *respondent's* policy pertaining to the use of third-party e-mail accounts or third-party storage devices or storage services (in other words, storage devices or services not provided or controlled by *respondent*) for business purposes.

11) Describe for me *respondent's* capability to directly access storage devices (including, but not limited to, desktop and/or laptop computers) through the company network, including, but not limited to, synchronization capability between different types of storage devices and/or network servers.

12) Describe for me *respondent's* capability for accessing mobile devices issued to employees or used by its employees under *respondent's* "BYOD" policy.

13) Describe any third-party messaging systems used by *respondent* or "unofficially" by employees in *[business unit*] for business purposes, such as Facebook, LinkedIn, Snapchat, Instagram, Weibo (Sina Weibo), Twitter, Voxer, Yammer, Chatter, or similar systems.

Retrieval Systems, Capabilities, and Practices

14) Describe for me *respondent's* record retention policy, including, but not limited to, *respondent's* retention policy concerning ESI and/or the way that *respondent's* records retention policy is applied to ESI and backed-up and/or archived ESI.

15) Describe for me *respondent's* process when responding to discovery, preservation or production demands or orders involving storage devices or services and/or ESI, including but not limited to the steps that are taken to preserve an electronic data backup set if so requested/ordered.

16) Describe for me the steps that *respondent* takes to preserve and/or recover the ESI of an employee of *respondent* upon termination of employment.

17) What is *respondent's* process followed when disposing of or recycling storage devices?

18) Describe *respondent's* method or system for tracking the use of storage devices such as barcode, serial number or other inventory control systems.

19) Describe *respondent's* process for backing up storage devices and networks including, but not limited to, the frequency with which data from storage devices and/or networks is backed up, and how backup media is stored both internally and, where applicable, with third parties.

20) What are *respondent's* policies and procedures regarding media re-use, including erasure of previously written datasets and the number of times media is re-used before being discarded?

21) Describe *respondent's* backup device naming, indexing, control, and/or numbering system or policy.

22) Describe the brands and versions of backup software used during the relevant time period and presently, the operating system brand and version on which backup software was running during the relevant time period and presently, the date of commencement of the present backup system, the brand and model of backup hardware in use for the backup system during the relevant time period and presently, and the business units that utilize the backup system.

23) Describe all steps that *respondent* takes to archive and/or preserve ESI stored remotely (e.g. in a "cloud" based service) including ESI stored in a third-party messaging system.

Data Preservation In This Case

24) Tell me about all actions or steps taken by *respondent* to preserve documents and ESI relating to the above-captioned matter

25) Who was involved in formulating and/or communicating any "hold" or similar notice to preserve?

26) Who was directed to preserve any documents and ESI through the "hold" or by other means?

27) Describe any deletion or destruction of *respondent's* documents or ESI that has taken place since *date.*