Paralegals and Lawyers: A Critical Partnership for Pretrial Litigation

TABLE OF CONTENTS

Presentation by Jennifer A. Dietz, Esq.
Law Offices of Jennifer A. Dietz, LLC
3225 South MacDill Avenue
Suite 129-297
Tampa, Florida 33629
813-789-8029
jdietz@jenniferdietz.com

Creating the Trial Notebook

1. Client intake information
2. Voir dire
3. Opening statement
4. Order of proof
5. Key pleadings (complaint, answer and affirmative defenses, counterclaims, etc.)
6. Key witness deposition summaries (one to two page summaries with page numbers correlating to pertinent facts)
7. Interrogatories
8. Answers to interrogatories
9. Requests for production of documents
10. Responses to requests for production of documents
11. Request for admissions
12. Responses to requests for admissions
13. Pretrial stipulations (court's and all parties)
14. Motions in Limine (all parties)
15. Opposing parties' responses to motions in Limine
16. Research and case law
17. Witness questions (all parties' witnesses)
18. Cross-examination questions (all parties' witnesses)
19. Summary of damages
20. Offers of judgment/settlement proposals
21. Closing argument
22. Jury instructions
23. Verdict form
24. List of all witnesses' full names, telephone numbers, and other critical information

*Note: Make five copies of each pertinent document, collate, and staple prior to trial for easy access.

Checklists for Pre-Suit Demand Packages

Automobile negligence claims and personal injury claims are usually time-consuming and frustrating to the solo practitioner and his/her paralegal. There are many documents and records that must be requested before you can even begin drafting a pre-suit demand letter. Once you have the necessary documents, organizing the materials relevant to the client's claim may take several hours, even after the final narrative report is received from the primary treating physician. In an effort to streamline the process and help utilize your time to the fullest, I offer the following checklist to be used as a guideline:

CLIENT PRE-SUIT CHECKLIST:

1. Accident Report
2. Signed medical authorizations for client
3. Client's auto insurance info
4. Defendant's auto insurance info
5. Citation disposition
6. Repair estimates
7. Photographs (accident scene, auto and personal)
8. Wage loss info
9. Ambulance Run Report
10. Hospital records
11. Doctor's records (including a Final Narrative Report)
12. Medical Bills (including prescriptions)
13. PIP payout ledger (client's auto insurance)
14. Other health insurance coverage info
15. Client's personal info (married, children, date of birth, Social Security Number)
16. Client's income tax returns for last 3 years

The above information in your file will enable you to prepare the most in-depth demand letter to the insurance carrier, and you will be rewarded by a quick turn-around offer of the policy limits available for your client's injury.

Here is another time-saving sample cover sheet to keep in the front of your client's file:

CLIENT INTAKE INFORMATION

DATE OF ACCIDENT:

BRIEF DESCRIPTION: *(e.g., auto accident, or slip-and-fall)*

CLIENT NAME AND ADDRESS:

TELEPHONE:

DOB:
SSN:

INSURANCE COMPANY:

LIMITS:

ADJUSTER & PHONE:

COMMENTS:

***

DEFENDANT NAME AND ADDRESS:

DEF. INSURANCE COMPANY:

LIMITS:

ADJUSTER & PHONE:

COMMENTS:

For the seasoned attorney and/or paralegal who has done several of these pre-suit packages, the above checklists will also help you be prepared for any pre-suit mediation that may be requested. (And of course, if all else fails, you will have all the necessary materials at hand to commence litigation!)

Document Requests: Drafting and Serving the Request (FL)

A Practice Note explaining how to draft and serve a request for production of documents (also known as an RFP, document request, or inspection demand) in a Florida civil suit. Specifically, this Note discusses the structure and content of a request for the production, and how to draft the different sections of a request for production, including the caption, introduction, instructions, definitions, document requests, and signature block. This Note also discusses the rules for serving the request for production and preparing a certificate of service.

Contents

A **request for the production** (RFP) is a formal, written **discovery** request that is used to obtain relevant, non-privileged documents, tangible things, and **electronically stored information** (ESI) from any party to a case (Fla. R. Civ. P. 1.350). An RFP may also request the inspection of land or other property controlled by a party, or to inspect, copy, test, or sample any tangible things within the scope of discovery (Fla. R. Civ. P. 1.350(a)). Counsel should carefully draft the RFP to obtain the

needed discovery and avoid unnecessary objections. This Note discusses key issues to consider when drafting and serving an RFP.

To obtain documents or other materials from a non-party, counsel must serve the non-party with a subpoena *duces tecum*. For information on obtaining documents from a non-party using a subpoena *duces tecum*, see Practice Note, Subpoenas in State Court: Drafting a Subpoena (FL).

Drafting the RFP

RFPs generally are broken down into the following sections:

- Caption and title.
- Introduction.
- Definitions.
- Instructions.
- Document requests.
- Signature block.
- Certificate of service.

RFP's are generally not filed with the court, and are therefore not subject to Florida's formatting rules (see Do Not File the RFP With the Court). Nonetheless, attorneys generally choose to follow these rules.

Caption and Title

Although it is not filed with the court, the RFP should contain a caption at the top of the first page that includes:

- The name of the court.
- The first-named plaintiff and defendant, followed by "*et al.*" if there are additional parties.
- The case number.

(Fla. R. Civ. P. 1.100(c)(2), (c)(5).)

The RFP title generally appears immediately below the caption, describes the request type, and identifies the party making the request (for example, "Defendant [DEFENDANT'S NAME]'s First Request for Production of Documents to Plaintiff [PLAINTIFF'S NAME]") (Fla. R. Civ. P. 1.100(c)(2), (c)(5)).

Introduction

Following the title, an RFP typically has an introductory statement that identifies:

- The party making the request.
- The party to whom the RFP is directed.
- A short statement of the nature of the request, such as:
  - the production of documents and ESI for inspection and copying,

- the production of tangible things for inspection, copying, testing, or sampling; or
- to permit entry upon designated land or other property.

Definitions

An RFP contains a section for definitions, including:

- Standard terms that are not specific to the case.
- Case-specific terms.

Typically, this section is formatted in consecutively numbered paragraphs.

Why Include Definitions?

Definitions make an RFP easier to understand. They also help prevent the producing party from objecting to or avoiding production of documents. Definitions should not be included for every term, but instead should be reserved for those terms that require explanation, such as to:

- Explain terms that otherwise might be ambiguous and subject to interpretation.
- Ensure that counsel receives all of the documents requested.
- Prevent the producing party from avoiding the production of documents with an overly narrow or literal interpretation of document requests.
- Simplify the requests and avoid confusion.

Definitions Should be Tailored

Although counsel may be tempted to recycle definitions from RFPs in other cases, RFP definitions must be tailored for each case to ensure clarity and relevance. However, RFPs from similar cases can be a good reference when drafting an RFP.

Definitions should be broad enough to cover the relevant information that counsel seeks. Counsel should selectively determine what terms should be defined. In the spirit of cooperation and to avoid discovery disputes and judicial intervention, each definition should be carefully crafted so it is not overly broad or vague rendering requests using that term objectionable.

Standard Definitions

Many standard terms are repeated throughout an RFP. Some examples of definitions that typically appear in RFPs are set out below:

- **Documents.** "The term 'document' means any book, paper, record, or other data, whether written, typed, electronically stored, recorded, or graphic of any kind or description, including originals, non-identical copies, and drafts, and includes all materials within the scope of Florida Rule of Civil Procedure 1.350(a) that are now or were at any time in the possession, custody, or control of the producing party."
- **Control.** "A person is deemed in control of a document if he has ownership, possession, or custody of a document, or the right to secure a document or a copy from any person or public or private entity with physical possession of the document." (See *Saewitz v. Saewitz*, 79 So. 3d 831, 834 (Fla. 3d DCA 2012).)
- **Communication.** "The term 'communication' means any form of correspondence, instruction, publication, contact, discussion, report, or written, electronic, or recorded oral exchange between two or more persons."

- **Relate or relating (or concern or concerning).** "Consisting of, referring to, reflecting, or being in any way logically or factually connected with the matter."
- **And/or.** "The terms 'and' and 'or' shall be construed either conjunctively or disjunctively as necessary to bring within the scope of the request any document, ESI, or tangible thing that might otherwise fall outside its scope."
- **All, any, or each.** "The use of 'all,' 'any,' or 'each' encompasses any and all of the matter discussed."
- **Number.** "The use of singular form includes plural and vice versa."
- **Tense.** "The use of present tense includes past tense and vice versa."

Define the Parties

Counsel should define to whom the RFP is directed (sometimes defined as "You"). For example, a definition for a corporate party subject to the RFP (or a corporate nonparty referenced in an RFP) might look like this:

- "'**XYZ**' or '**You**' means XYZ, Inc., its subsidiaries, divisions, predecessor and successor companies, affiliates, parents, any joint venture to which it may be a party, and/or each of its employees, agents, officers, directors, representatives, consultants, accountants and attorneys, including any person who served in any such capacity at any time during the relevant time period specified herein."

Other Case-Specific Terms

Counsel should define terms specific to the case, which might include terms such as the following examples:

- **Terms that are repeated throughout the RFP.** "The 'Collision' refers to the auto collision involving Plaintiff and Defendant that occurred on July 4, 2013, at the intersection of Main and First Streets in Orlando, Florida."
- **Vague or cumbersome terms.** "The 'Convention' means the Convention on the Settlement of Investment Disputes between States and Nationals of Other States, submitted to Governments by the Executive Directors of the International Bank for Reconstruction and Development on March 18, 1965, which entered into force on October 14, 1966."
- **The case.** "'Litigation' refers to *Jack Smith v. ABC, LLC*, Case No. 14-00923, pending in the Eleventh Judicial Circuit in and for Miami-Dade County, Florida."
- **Abbreviated terms.** "'SEC' refers to the U.S. Securities and Exchange Commission."
- **Documents for which drafts or prior iterations of a final version are sought** (in addition to the final version itself), such as:
  - **relevant agreements or corporate documents.** "'Financial Statements' refer individually and collectively to [COMPANY]'s annual financial statements for fiscal years ending [DATE];" or
  - **relevant public filings and financial statements.** "'SEC Registration Documents' refer to the first registration statement filed by [COMPANY] on [DATE], and the subsequent amendments through Form registration statement dated [DATE]; and Form registration statement dated [DATE], all of which were filed with the SEC."

Instructions

Instructions govern the producing party's response to the RFP. As with the definitions, the instructions should be clear and fully reflect counsel's directives for the response. Typically, this section is formatted in consecutively-numbered paragraphs.

Why Include Instructions?

The instructions direct the mechanics of how a producing party should respond to an RFP. They put the producing party on notice regarding the requesting party's expectations for responses to the RFP. Counsel should include clear instructions to help ensure that they receive the information they request and in the form they want.

What Instructions Should Be Included?
The instructions in the RFP should be consistent with the Florida Rules of Civil Procedure, the court's local rules administrative orders, and the judge's individual practice rules. At a minimum, the following general instructions should be included in every RFP:

- **Applicable time period.** "Unless otherwise stated, all documents requested are for the period beginning [DATE] up to and including [DATE]."
- **Privileged and protected documents.** "If any document or other requested information is withheld because of a claim of privilege or protection, such as the attorney-client privilege, the work-product doctrine, or trade secret, the producing party shall set forth separately with respect to each document:
  - the ground of confidentiality claimed;
  - each and every basis under which the document is withheld;
  - the type of document;
  - the document's general subject matter;
  - the document's date; and
  - any other information to enable an assessment of the applicability of the privilege or protection as required by Florida Rule of Civil Procedure 1.280(b)(6)."

Other Instructions to Include
For additional clarity, counsel may choose to include additional instructions, such as:

- **How to handle redacted documents.** "To the extent [PRODUCING PARTY] asserts that a document contains confidential or sensitive information that should be protected from disclosure (based on the attorney-client privilege, work product doctrine, or another protection) and non-privileged information, the non-privileged portions of the document must be produced. For each such document, indicate the portion of the document withheld by stamping the words 'MATERIAL REDACTED' on the document in an appropriate location that does not obscure the remaining text."
- **Producing documents in their entirety.** "Each request contemplates production of all documents in their entirety. If a portion of a document is responsive to one or more requests, the document shall be produced in its entirety."
- **Organizing the document production.** "All documents are to be produced as they are kept in the usual course of business with any identifying labels, file markings or similar identifying features, or shall be organized and labeled to correspond to the categories requested herein."
- **Identifying whether the producing party has no responsive information, or has withheld information.** "If there are no documents in response to any particular request, or if you withhold any responsive information or categories of information based on any objections, [PRODUCING PARTY] shall state so in writing."

The Florida Rules of Civil Procedure do not require a producing party to supplement a response to a request for discovery with after-acquired documents, information, or things if the party's response was complete when made (Fla. R. Civ. P. 1.280(f)). Therefore, a requesting party should consider making additional requests if it suspects that a responding party has possession of such after-acquired information.

Instructions for Producing ESI

Florida Rules of Civil Procedure 1.350 and 1.280(b)(3) specifically permit discovery of ESI and allow:

- The requesting party to specify the form in which the ESI is to be produced.
- The producing party to:

- object to producing the ESI in the form the requesting party requests;
- produce the requested ESI in the form in which it is ordinarily maintained; or
- produce the requested ESI in a reasonably usable form.

(Fla. R. Civ. P. 1.350(b) and 1.280(b)(3).)

To avoid unnecessary delay and motion practice, the party requesting ESI should simply provide an instruction for the manner of producing any ESI. An example of an instruction for production of ESI might be as follows:

- "You must produce electronic or magnetic data responsive to these requests in the form in which the data is ordinarily maintained, or in a form that is reasonably usable and able to be stored or recovered with all metadata intact."

Specific forms of ESI that can be requested for production include:

- **Native files**.
- **PDFs**.
- **TIFFs** and **load files**.
- **Metadata**.

For more information on e-discovery in Florida, see Practice Note, E-Discovery in Florida: Overview.

Native Files

A native file is an electronic document stored in the form in which it was created. In e-discovery, if documents are produced in their native form, the original software application might be needed to view the document (for example, a document created by word processing software might only be viewable on a computer with that software).

Typically, native files contain metadata (see Metadata). For this reason, document production of native files is particularly useful for production of spreadsheets and Microsoft PowerPoint presentations that may contain notes or formulas that will not appear to the reader if the document is converted to another file format or printed.

Documents in their native format have lower processing costs than images, such as PDFs or TIFFs because there is less processing needed (native files already are searchable and should have their metadata intact). However, document review of native files may be more time-consuming.

The requesting party may prefer native file format because it enables counsel to:

- Search each document.
- Review formulas and hidden text.
- Access metadata.
- Set the print area.

However, native files tend to be more difficult to handle in litigation because they:

- Generally are more time consuming to review because each document reviewed first must be opened in the native software.
- Are at risk for spoliation of metadata if not reviewed on a document review database that preserves the metadata.
- Will not have a visible **Bates number**, so they are more difficult to identify as evidence at a deposition or at trial.
- Cannot be redacted. As a result, native files requiring redaction commonly are produced in PDF or TIFF format.
- May be more difficult to authenticate.

An example of an instruction requesting ESI in native format follows:

"You must produce ESI responsive to these requests in its native format, along with each file's accompanying metadata, as follows:

- documents created using Microsoft Word must be produced as .doc or .docx files;
- documents created using Microsoft Excel must be produced as .xls or .xlsx files; and
- emails must be produced as .msg or .pst files."

PDFs

A PDF is designed to capture the entirety of a document, including any text and images contained in the document. PDFs may also contain features added by the creator of the document, such as hyperlinks. PDFs are easy to:

- Search.
- Bates stamp.
- Redact.

PDFs typically are the preferred static form for document production. However, PDFs might not be preferred by counsel concerned with:

- Metadata, since not all metadata is preserved when electronic files are converted to PDF.
- The appearance of cumbersome documents, such as spreadsheets.
- The costs associated with converting files to PDF and for **optical character recognition** (OCR) or text extraction.

An example of an instruction requesting ESI in PDF format (which includes a fallback instruction for production of native files) follows:

- "You must produce electronic or magnetic data responsive to these requests in text-searchable PDF format with corresponding load files that contain the document's text, including all metadata pertaining to the files that contain such data. Any files that are not easily converted to PDF format, such as spreadsheet, database and drawing files, should be produced in native format."

TIFFs and Load Files

TIFF (also known as TIF) is an acronym for Tagged Image File Format. A TIFF is an electronic file copy of a paper document, which contains no embedded text, fonts, or graphics. Basically, a TIFF file is a picture of how a document looks. TIFF images cannot be searched for text and they do not contain metadata. Files in TIFF format often end with a .tif extension. They can be single or multi-page. Examples of TIFF files include:

- Scanned documents.
- Received faxes.

Because TIFF files are unsearchable, a request for TIFF files in a document production typically includes load files, which contain metadata as well as searchable text identified through OCR software. A load file is a text or data file containing data about each TIFF image in a particular document production. The load file is loaded onto a database so that counsel can search the data associated with each processed file, which is linked to a corresponding TIFF image. Load files typically:

- Contain the text of each document, using OCR.
- Include Bates numbers.
- Identify the document custodian.

- Include extracted data including email sender and recipient information.

Historically, TIFF images were widely used for document production. Today, PDF files are used more often than TIFF files in document productions because PDFs have greater functionality than TIFFs, including that PDF files generally are searchable.

TIFF images might not be preferred by counsel because:

- The available metadata is limited.
- Cumbersome documents, such as spreadsheets, are difficult to view.
- Files may require conversion to utilize OCR for search purposes.
- OCR is dependent on image quality and may not be effective, therefore limiting searchability.

Metadata
Metadata is information, often hidden, that describes the history, tracking, or management of an electronic file, such as:

- File name and/or title.
- The location or path where the file was stored.
- Size.
- Subject.
- Comments or notes.
- Author.
- Persons who have reviewed or edited the file.
- Persons who have permission to access the file.
- Dates of creation and modification.
- Dates of most recent printing, access, and metadata modification.
- Total editing time.

Metadata may be created automatically by a computer system or manually by a user. Where copies of disclosed documents are provided in native format, some metadata is typically disclosed with each document.

Metadata may be available for viewing on a **document review platform**, in a load file, or in the document properties, depending on how counsel is viewing the documents. Apart from the direct value of the information, metadata may also be helpful for authenticating documents.

Document Requests

The actual document requests are contained in the body of the RFP, following the definitions and instructions. The document requests contain specific requests for documents and information. This section should be formatted in consecutively-numbered paragraphs. The responding party must generally identify the produced documents or things to correspond with the categories in the request or produce them in the way they are kept in the usual course of business (Fla. R. Civ. P. 1.350(b)).

Considerations When Drafting Specific Requests
Counsel should make discovery requests that:

- Comply with Florida Rules of Civil Procedure and any rules, orders, stipulations, or agreements in the case.

- Are consistent with existing law or are supported by a good faith argument for the extension, modification, or reversal of existing law.
- Are relevant to the subject matter, claims, and defenses of the pending action.

In Florida, requests for production, inspection, or entry must be:

- Made in a pending action (*Epstein v. Epstein*, 519 So. 2d 1042, 1043 (Fla. 3d DCA 1988)).
- Relevant to the subject matter of the action (*Friedman v. Heart Inst. of Port St. Lucie*, Inc., 863 So. 2d 189, 194 (Fla. 2003).)
- Made to a party that has possession, custody, or control of the items or property (Fla. R. Civ. P. 1.350(a)(1)).

Counsel should not make discovery requests that are:

- Asserted for an improper purpose, such as to harass or to cause unnecessary delay or expense.
- Unreasonable, unduly burdensome, or expensive.
- Frivolous.

(FL ST BAR Rule 4-3.4; *Elkins v. Syken*, 672 So. 2d 517, 522 (Fla. 1996).)

Think About Claims and Defenses

Counsel should draft document requests to obtain information needed to prosecute or defend the case. When drafting requests, counsel should consider what documents may exist that:

- Are relevant to the subject matter in the case (*Friedman v. Heart Inst. of Port St. Lucie*, Inc., 863 So. 2d 189, 194 (Fla. 2003)).
- Prove or disprove allegations in the pleadings.
- Support or refute the elements of the claims or defenses in the pleadings or dispositive motion papers.
- Bolster or discredit potential witnesses (*Steinger, Iscoe & Greene, P.A. v. GEICO Gen. Ins. Co.*, 103 So. 3d 200, 206 (Fla. 4th DCA 2012)).

One strategy that counsel might use to prepare effectively targeted document requests is to:

- Prepare the jury instructions that need to be proven to successfully prevail on the merits of the case (even if counsel anticipates a non-jury trial).
- Study the elements of the causes of action or defenses.
- Evaluate the specific evidence needed to establish each element of the causes of actions or defenses.
- Draft the document requests accordingly.

Information Available Through Requests for Production

Parties may request any non-privileged documents that are relevant to the subject matter of the pending action, whether they relate to the claims or defenses of the requesting party or the claims or defenses of any other party to the action (Fla. R. Civ. P. 1.280(b)(1)).

Florida Rule of Civil Procedure 1.280(b)(4) allows a party to obtain discovery of work product (that is, documents and tangible things otherwise discoverable under Rule 1.280(b)(1), but prepared in anticipation of litigation or trial) **only** upon a showing that the party seeking discovery:

- Needs the materials in the preparation of the case.

- Is unable without undue hardship to obtain the substantial equivalent of the materials by other means.

(Fla. R. Civ. P. 1.280(b)(4).)

Requests Should be Tailored

Counsel must consider the purpose of each request. The producing party may construe an RFP as narrowly and literally as possible in order to limit the information produced in response to the request, so counsel must draft document requests that are sufficiently broad enough to capture the pertinent information.

On the other hand, the producing party might apply an expansive interpretation to a discovery request. This may lead to an objection that the request is overbroad or not reasonably limited in time and scope. The producing party might also produce a very large amount of irrelevant (but technically responsive) documents on the requesting party to slow down the review or delay the case. Therefore, all requests should be reasonably tailored to include only matters relevant to the case.

What Documents Should Counsel Request?

There are certain types of documents that may be helpful for counsel to prepare their case regardless of the underlying subject matter. Where applicable, counsel may want to request:

- **Document retention policies.** Counsel should request the producing party's document retention policy to ensure that the producing party searches all available sources of information when responding to the RFP.
- **Settlement agreements.** Counsel should request the production of settlement agreements if they suspect that a party may have entered into settlement agreements in connection with the facts underlying the case (for example, settlement agreements with insurers).
- **Evidence of insurance coverage.** Plaintiff's counsel should know if the possibility of insurance coverage plays into the litigation. Insurance agreements are within the scope of discovery. (Fla. R. Civ. P. 1.280(b)(2).)
- **Joint defense agreements.** If counsel suspects that some or all of the defendants in a case are working together, it may be advisable to request the production of joint defense agreements.

What Documents Should Not Be Requested?

Counsel is not entitled to every document in the possession of the producing party. Rather, disclosure is limited to relevant, non-privileged documents, information, or tangible things. (Fla. R. Civ. P. 1.280(b)(1).) Certain document requests are usually deemed to be improper under Florida law. For example:

- **Overly-broad requests**. Counsel should avoid making overly-broad requests for things like "all correspondence, instructions, memos, orders, sheets, worksheets" without a reasonable subject matter limitation (*Life Care Ctrs. of Am. v. Reese*, 948 So. 2d 830, 832 (Fla. 5th DCA 2007)).
- **Attorney work product.** Requests for production in a particular manner or of particular documents in circumstances that would reveal the opposing lawyer's mental impressions violate the work product privilege (*Northup v. Acken*, 865 So. 2d 1267, 1272 (Fla. 2004)). Counsel may, in good faith, seek work product only by showing that a substantial need for the information and inability to obtain its substantial equivalent without undue hardship (Fla. R. Civ. P. 1.280(b)(4)).
- **Privileged documents.** Counsel should not request specifically identified documents that are obviously protected by the attorney-client privilege or some other recognized privilege or protection unless she has reasonable grounds to believe the privilege or protection has been waived.
- **Frivolous discovery requests.** Florida attorneys are specifically prohibited from "making a frivolous discovery

request" (FL ST BAR Rule 4-3.4).

- **Documents already in the possession, custody, or control of the requesting party.** Typically, counsel should not request documents already in the requesting party's possession or control **unless** it is relevant to the case that a particular document was held in the producing party's files as evidence that the producing party:
  - created the document;
  - edited the document;
  - had access to or viewed the document; or
  - had possession of the document.
- **Information that the requesting party does not want to produce.** A request for sensitive information leaves the requesting party susceptible to a retaliatory request for the same type of information (for example, production of customer or client lists and documents that were created after the litigation began).

Properly Phrase the Requests

Because the requests should put the producing party on notice of the documents sought, they should be clear, and not confusing or vague. Below are examples of properly worded document requests compared to objectionable requests.

Proper Request	Objectionable Request
Breach of contract: mitigation of damages. All documents relating to efforts by plaintiff to obtain an alternative buyer for the product.	**Breach of contract: mitigation of damages.** All documents concerning mitigation of damages. (Possible objections include: vague, overly broad if the relevant time period is not defined, not reasonably calculated to lead to the discovery of admissible evidence.)
Personal jurisdiction: alter-ego. All documents relating to the formation of the company.	**Personal jurisdiction: alter-ego.** All corporate documents concerning the company. (Possible objections include: overly broad, vague, unduly burdensome, not reasonably calculated to lead to the discovery of admissible evidence.)
Antitrust: parallel conduct. All documents relating to meetings or communications with other defendants concerning the allocation of customers for the product.	**Antitrust: parallel conduct.** All documents concerning meetings or communications with other defendants. (Possible objections include: overly broad, unduly burdensome, not reasonably calculated to lead to the discovery of admissible evidence.)

Signature Block

Counsel must sign the RFP and include a signature block that contains counsel's:

- Name.
- Mailing address.
- Telephone number, including area code.
- Email address (and secondary email addresses, if applicable).
- Florida Bar number (or notice that counsel is admitted **pro hac vice**).

(Fla. R. Jud. Admin. 2.515(a).)

While not required, the signature block also usually includes the following:

- Counsel's law firm name.
- Counsel's fax number.
- The name of counsel's client.

An electronic signature (that is, typing "/s/," "/s," or "s/" followed by the signing attorney's name on the signature line) is acceptable for documents served by email (Fla. R. Jud. Admin. 2.515(c)(1)(C)).

For more information on signatures in Florida court documents, see Practice Note, General Formatting Rules in Circuit Court (FL): Signatures. For a sample signature block, see Standard Clause, Circuit Court Signature Block (FL).

Certificate of Service

A certificate of service should be included in the RFP below the signature block (Fla. R. Jud. Admin. 2.516(f)). It constitutes **prima facie** proof that the RFP was served on the parties identified in the certificate (Fla. R. Jud. Admin. 2.516(f)).

The certificate of service should contain:

- A description of the document served.
- The names of the attorneys served.
- The method of service.
- The names of the law firms of the attorneys served.
- The address used for service (that is, email address, fax number, or mailing or delivery address).
- The mailing address, if different from the service address.
- The date of service.
- Serving counsel's signature. For e-filed documents, counsel should use an electronic signature (that is, "/s/" followed by the signing attorney's name).

(Fla. R. Jud. Admin. 2.516(f).)

For more information on certificates of service, see Practice Note, General Formatting Rules in Circuit Court (FL): Proof of Service. For a sample certificate of service that may be used in Florida court documents, see Standard Clause, Certificate of Service (FL).

Serving the RFP

Before serving the RFP, counsel should review the court's local rules, administrative orders, and the judge's individual practice rules to ensure proper service.

For additional information on serving Florida court documents, see Practice Note, Serving Interlocutory Documents (FL).

Serve All Parties

Counsel must serve RFPs on all parties to the case, not just the party to whom the requests are directed. The request may be served:

- On the plaintiff, after commencement of the action.
- On the defendant, after service of the process and initial pleading on that party.

(Fla. R. Civ. P. 1.350(b).)

Do Not File the RFP With the Court

Because Rule 1.350(b) only requires service, RFPs are typically not filed with the court unless one of the following applies:

- The court has ordered discovery to be filed.
- The discovery is attached as an exhibit to a motion or other court filing.
- The discovery is necessary for a hearing or an appellate proceeding.

Documents produced in discovery are not filed unless required by the court (Fla. R. Civ. P. 1.280(g) and 1.350(d)).

Method of Service

There is a split of authority over whether the email service requirement in Florida Rule of Judicial Administration 2.516(b)(1) applies to a document served but not filed with the court, such as an RFP (see *Wheaton v. Wheaton*, 2017 WL 608523 at *2 (Fla. 3d DCA Feb. 15, 2017) (email service required); but see *Boatright v. Philip Morris USA Inc.*, 2017 WL 1363915 at *7 (Fla. 2d DCA Apr. 12, 2017) (email service not required)).

Despite the split of authority, the best practice is to always serve a notice of party deposition by email in compliance with the email formatting requirements of Rule 2.516(b), which require that:

- The subject line of the email contain the language: "SERVICE OF COURT DOCUMENT Case No. [CASE NUMBER]."
- The body of the email identifies:
  - the court;
  - the case number;
  - the first-named party on each side;
  - the titles of the documents being served; and
  - the name and telephone number of the person serving the documents.
- (Fla. R. Jud. Admin. 2.516(b)(1)(E).)

Failure to follow these rules may render the email service ineffective (*Matte v. Caplan*, 140 So. 3d 686 (Fla. 4th DCA 2014)).

Document Requests: Request for the Production of Documents (RFP) (FL)

A sample request for the production of documents that may be used in civil litigation in Florida. This Standard Document has integrated drafting notes with important explanations and drafting tips.

IN THE CIRCUIT COURT OF THE [NUMBER] JUDICIAL CIRCUIT
IN AND FOR [COUNTY NAME] COUNTY, FLORIDA

[NAME],
Plaintiff[s],
vs.
[NAME],
Defendant[s].
_____/

Case No. [NUMBER]

[PLAINTIFF/DEFENDANT] [NAME]'S [NUMBER] REQUEST FOR THE PRODUCTION OF DOCUMENTS TO [DEFENDANT/PLAINTIFF] [NAME]

[Plaintiff/Defendant], [NAME OF REQUESTING PARTY], pursuant to Florida Rule of Civil Procedure 1.350, requests that [Defendant/Plaintiff], [NAME OF PRODUCING PARTY], produce the following documents within [30/45] days of the date of service hereof at [LOCATION].

DEFINITIONS

1. [["NAME OF CORPORATION,"] "You," or "Your" means [defendant/plaintiff], [NAME OF CORPORATE PRODUCING PARTY], its subsidiaries, divisions, predecessor and successor companies, affiliates, any partnership or joint venture to which it may be a party, and its employees, agents, officers, directors, representatives, consultants, accountants, and attorneys, including any person who served in any such capacity at any time during the relevant time period specified herein.

OR

["NAME OF INDIVIDUAL,"] "You," or "Your" shall mean [defendant/plaintiff], [NAME OF INDIVIDUAL PRODUCING PARTY], [his/her] employees, agents, officers, directors, representatives, consultants, accountants, attorneys, and any other person or entity acting or purporting to act on [his/her] behalf, including any person who served in any such capacity at any

time during the relevant time period specified herein.]

2. The term "document" means any book, paper, record, or other data or data compilations, whether written, typed, printed, electronically stored, recorded, or graphic of any kind or description, including originals, non-identical copies, and drafts, and includes all materials within the scope of Rule 1.350(a). The term "document" refers to any document now or at any time in the possession, custody, or control of the producing party.

3. A person is deemed in "control" of a document if he has ownership, possession, or custody of a document, or the right or ability to secure a document or a copy thereof from any person or public or private entity with physical possession of the document.

4. A reference to a person includes an individual, corporation, partnership, joint venture, limited liability company, governmental authority, unincorporated organization, trust, association or any other form of public, private, or legal entity and includes all of that person's principals, employees, agents, officers, directors, attorneys, consultants and other representatives.

5. The "Action" shall mean this proceeding, captioned [NAME OF PLAINTIFF] v. [NAME OF DEFENDANT], Case No. [NUMBER], currently pending in the [COURT].

6. The term "communication" means any form of correspondence, instruction, publication, contact, discussion, report, or written, electronic, or recorded oral exchange between two or more persons.

7. ["Relate" or "relating"/"Concern" or "concerning"] means consisting of, referring to, reflecting, or being in any way logically or factually connected with the matter.

8. The terms "and" and "or" shall be construed either conjunctively or disjunctively as necessary to bring within the scope of the request any document, ESI, or thing that might otherwise fall outside its scope.

9. The terms "all," "any," or "each" encompass any and all of the matter discussed.

10. The use of singular form includes plural, and vice versa.

11. The use of present tense includes past tense, and vice versa.

12. [INSERT ADDITIONAL DEFINITIONS].

INSTRUCTIONS

1. All documents must be produced as they are kept in the usual course of business with any identifying labels, file markings, or similar identifying features, or shall be organized and labeled to correspond to the categories requested herein.

2. [You must produce electronically stored information (ESI) in its original native format, with all metadata intact. For example:

- Documents created using Microsoft Word must be produced as .doc files
- Emails must be produced as .msg or .pst files.
- [ADDITIONAL PRODUCTION SPECIFICATIONS].

OR

You must produce electronically stored information (ESI) in text-searchable PDF format with corresponding load files containing the document's text and all available metadata. Any files that are not easily converted to text-searchable PDF format, such as spreadsheet, database and drawing files, should be produced in native format.]

3. Unless otherwise stated herein, the relevant time period for all requested documents, information, and things is the period commencing [DATE] up to and including [DATE].

4. These requests call for the production of all responsive documents, information, or tangible things in your possession, custody, or control, or in the possession, custody, or control of your employees, predecessors, successors, subsidiaries, divisions, affiliates, partners, joint venturers, brokers, accountants, financial advisors, representatives and agents or other persons acting on your behalf, without regard to the physical location of such documents.

5. In responding to these requests, include documents, information, or things obtained on your behalf by your counsel, employees, agents, or any other persons acting on your behalf. If your response is that the requested item is not within your possession or custody, describe in detail the unsuccessful efforts you made to locate each such item. If your response is that the requested item is not under your control, identify who has the control and the location of each requested item.

6. If any document, information, or tangible thing was, but no longer is, in your possession, custody, or control, or in existence, include a statement:

- identifying the item;
- describing where the item is now;
- identifying who has control of the item;
- describing how the item became lost or destroyed or was transferred; and
- identifying each of those persons responsible for or having knowledge of the loss, destruction, or transfer of the requested item from your possession, custody, or control.

7. Each request contemplates production of all documents in their entirety. If a portion of a document is responsive to one or more requests, the document shall be produced in its entirety.

8. If any document or other requested information is withheld, in whole or in part, by a claim of privilege, such as attorney-client privilege, work-product doctrine, or trade secret, the producing party shall set forth separately with respect to each document:

- the ground of confidentiality claimed;
- each and every basis under which the document is withheld;
- the type of document;
- its general subject matter;
- the document's date; and
- other information to enable an assessment of the applicability of the privilege or protection as required by Fla. R. Civ P. 1.280(b)(6).

9. To the extent you assert that a document contains information that should be protected from disclosure (based on the attorney-client privilege, work-product doctrine, or another protection), and non-privileged information, the non-privileged portions of the item must be produced. For each such document, indicate the portion of the document withheld by stamping the words "MATERIAL REDACTED" on the document in an appropriate location that does not obscure the remaining text.

10. If there are no documents, information, or tangible things in response to any particular request, or if you withhold any responsive information, you shall state so in writing.

11. [INSERT ADDITIONAL INSTRUCTIONS].

DOCUMENTS REQUESTED

REQUEST NO. 1: All documents received by you in response to any document requests or subpoenas propounded by [NAME OF PRODUCING PARTY] in this action.

REQUEST NO. 2: All documents referred to or quoted in the [complaint/answer/counterclaim].

REQUEST NO. 3: All documents relating to the allegations set forth in Paragraph [NUMBER] of the [complaint/counterclaim].

REQUEST NO. 4: All documents relating to the [allegations/response] in Paragraph [NUMBER] of the [complaint/answer/counterclaim] that [QUOTE ALLEGATION].

REQUEST NO. 5: [PRODUCING PARTY]'s electronic data and document retention policies for the relevant time period.

REQUEST NO. 6: All documents relating to the circumstances surrounding [PRODUCING PARTY]'s actual discovery of the facts underlying the allegations set forth in the [petition/answer/counterclaim].

REQUEST NO. 7: All documents reflecting, discussing, or relating to insurance coverage for this action.

REQUEST NO. 8: All documents that [PRODUCING PARTY] will or may introduce as evidence at trial in this action.

REQUEST NO. 9: [INSERT ADDITIONAL DOCUMENT REQUESTS].

Dated: [MONTH] [DAY], [YEAR]

Respectfully submitted,

[NAME OF LAW FIRM]

[STREET ADDRESS]

[CITY], FL [ZIP CODE]

[TELEPHONE NUMBER]

[FAX NUMBER]

By: /s/ [ATTORNEY NAME]

[ATTORNEY NAME]

Florida State Bar No.: [NUMBER]

[E-MAIL ADDRESS]

Attorney for [Plaintiff/Defendant] [NAME OF PLAINTIFF/DEFENDANT]

CERTIFICATE OF SERVICE

I hereby certify that this document was served via [the Florida Court E-Filing Portal/email/U.S. Mail/fax/hand delivery] on [DATE] upon: [ATTORNEY NAME(S)], counsel for [PARTY NAME], at [LAW FIRM NAME], [MAILING ADDRESS], [EMAIL ADDRESS(ES)].

/s [ATTORNEY NAME]

[ATTORNEY NAME]

Document Responses: First Steps in Responding to an RFP (FL)

This Practice Note describes the first steps that counsel should take when they expect to receive a request for the production of documents (RFP) under ***Florida Rule of Civil Procedure 1.350*** *in connection with a Florida state court lawsuit. This Note covers the steps that should be taken to preserve documents before an action begins, including complying with a document retention policy, implementing a litigation hold, and taking steps to avoid liability for spoliation, and the steps to take after a lawsuit is filed, including gathering documents and responding to the request for production. This Note also explains how to gather and produce electronically stored information (ESI), including file formats commonly available for productions (for example, native files, PDFs, TIFFs, load files, and metadata), how to search for and identify relevant ESI (including keyword and concept searches), coding of documents, and de-duplication.*

Contents

E

Modifying the Scope of Documents and ESI for Review
Duty to Supplement
Costs of Production

Documents and **electronically stored information** (ESI) play a significant role in almost every litigation. Parties to a Florida lawsuit generally serve a **request for production** of documents (RFP) under Florida Rule of Procedure 1.350 seeking relevant documents and other items from other parties. Counsel and clients should prepare to respond to an RFP as early as possible. This Note covers the process for responding to a document request, including:

- The steps to take before an action begins.
- How to respond to a document request after a lawsuit is filed.
- How to collect and produce electronically stored information.
- How to work with opposing counsel during the production process.
- The costs of production.

Before an Action Begins

Counsel should take steps to prepare for a potential document request as soon as the potential for litigation arises.

Staying Current with the Document Retention Policy

A company's **document retention policy** (also known as a document destruction policy) includes a schedule of how long the company retains documents based on the type of document and its subject matter. The retention policy typically requires the destruction of all records that have satisfied the retention requirements. A company should have a document retention policy long before any litigation is anticipated, so that the company routinely retains and regularly purges documents according to a set schedule.

The destruction of information pursuant to a valid document retention policy is not wrongful under ordinary circumstances (*Arthur Andersen LLP v. US*, 544 U.S. 696, 704 (2005)). Typically, an inference of bad faith will not be drawn if documents are routinely destroyed under a document retention policy. By staying current with its document retention policy, a company avoids the added expense of and risks associated with the production of documents that should no longer be in its possession.

A company that has a document retention policy should ensure that the policy is followed, meaning that the company regularly purges documents that it is no longer required to retain.

On the other hand, when complying with its document retention schedule, the company should ensure that records subject to a litigation hold are not inadvertently destroyed as part of regularly scheduled destruction.

For more information about document retention policies, see Practice Note, Drafting a Document Retention Policy.

Preserving Information

A party should start thinking about preserving information as soon as litigation is reasonably foreseeable. Because an RFP typically must be responded to within 30 days (or 45 days if served contemporaneously with the original complaint), waiting until an RFP is served gives the recipient little time to collect, review, and produce relevant documents and ESI to the requesting party (Fla. R. Civ. P. 1.350).

Though there is no common law duty to preserve evidence in anticipation of litigation in Florida, there may be a statutory or contractual duty to preserve evidence in certain instances (*Gayer v. Fine Line Constr. & Elec., Inc.*, 970 So. 2d 424, 429 (Fla. 4th DCA 2007)). For example:

- A Florida hospital has a statutory duty to make, retain, and provide copies of its patients' medical records to the patients or their representatives after discharge, upon request and payment (§ 395.3025, Fla. Stat.).
- Under certain circumstances, employers and employees have a statutory duty to preserve evidence relating to workers' compensation actions (§ 440.39(7), Fla. Stat.; *Gen. Cinema Beverages of Miami, Inc. v. Mortimer*, 689 So. 2d 276, 279 (Fla. 3d DCA 1995)).
- A duty to preserve evidence arises when a party is served with a discovery request (*Gayer v. Fine Line Constr. & Elec., Inc.*, 970 So. 2d 424, 429 (Fla. 4th DCA 2007)).

Avoiding Sanctions for Spoliation

If a company fails to produce requested, relevant, and non-privileged documents and ESI, it may risk sanctions for **spoliation** of evidence. In Florida, spoliation has been defined as the intentional destruction of evidence. When spoliation is established, the fact finder may draw an adverse inference that the evidence destroyed was unfavorable to the party responsible for the spoliation. (*Aldrich v. Roche Biomedical Labs., Inc.*, 737 So. 2d 1124, 1125 (Fla. 5th DCA 1999).)

The Florida Supreme Court has held that there is no independent cause of action in Florida against a first-party defendant for spoliation of evidence. Rather, there are available discovery sanctions, negative presumptions, and adverse inferences or jury instructions to deter a party from destroying or concealing of evidence in a civil matter. (*Martino v. Wal-Mart Stores, Inc.*, 908 So. 2d 342, 347 (Fla. 2005).)

Before allowing any remedy for a spoliation claim between parties, a Florida court must answer three questions:

- Whether the evidence existed at one time.
- Whether the spoliator had a duty to preserve the evidence.
- Whether the evidence was critical to an opposing party being able to prove its prima facie case or a defense.

(*Golden Yachts, Inc. v. Hall*, 920 So. 2d 777, 781 (Fla. 4th DCA 2006).)

While there is no common law duty to preserve evidence in Florida, the Second District Court of Appeal has held a duty to preserve evidence arises where a party makes a written request that the evidence be preserved (*Osmulski v. Oldsmar Fine Wine, Inc.*, 93 So. 3d 389, 395 (Fla. 2d DCA 2012)). The Fourth District has also noted that a duty to preserve evidence arises in certain cases where the defendant could have reasonably foreseen the claim (*Am. Hosp. Mgmt. Co. of Minn. v. Hettiger*, 904 So. 2d 547, 549 (Fla. 4th DCA 2005)).

Therefore, to avoid a possible finding of spoliation a company and counsel should preserve documents and ESI once they:

- Receive a plaintiff's demand letter.
- Receive a litigation hold notice.
- Have notice of a credible threat to sue.

Promptly Implementing a Litigation Hold

Because Florida common law does not impose a clear duty to preserve evidence in anticipation of litigation, reasonable efforts should be taken immediately to implement a litigation hold if a party or potential litigant receives a litigation hold notice regarding actual or suspected litigation. A company should also issue a formal written litigation hold to preserve documents and ESI if it receives notice of a governmental agency investigation, a subpoena, or court order seeking documents.

A litigation hold notice should:

- Be in writing.
- Identify the individuals who may have relevant information.
- Ask for the identity of any other individuals that may have relevant information who are not on the distribution list:
  - within the company; and
  - outside the company.
- Use plain English to:
  - define what information the recipients must preserve; and
  - explain how to preserve the information.
- Be sent from someone at the company with authority to ensure employee attention and compliance.

Counsel should maintain a litigation hold notice template ready to be tailored to the specific circumstances, which enables the client company to promptly implement a hold notice immediately upon learning about an actual or suspected litigation. In determining the scope of information that the company should preserve, counsel should consider what is reasonable given:

- The nature of the issues raised in the matter.
- The amount in controversy.
- Their experience in similar circumstances.

For additional information on implementing a litigation hold in Florida, see Practice Note, Implementing a Litigation Hold (FL).

Considering Third Parties that May Have Relevant Information

A party responding to a document request must consider all potential sources of responsive information in its possession, custody, or control (Fla. R. Civ. P. 1.350(a)). Determining who has control of a producing party's documents may be complicated because it may extend to third parties. For example, a party may be responsible for producing responsive information held by its:

- **Current employees**. A company is responsible for retrieving relevant documents held by its current employees. This includes any hard copy documents that are located in employees' homes and ESI stored on their personal devices, such as personal computers, laptop computers, tablets, cell phones, and PDAs.
- **Agents, contractors, and subcontractors**. A document in the possession of a party's attorney or agent may be deemed to be in the party's possession, custody, or control.
- **Parent companies, sister companies, and subsidiaries**. A parent company may have a sufficient degree of ownership and control over a wholly-owned subsidiary or sister company requiring producing of relevant documents and ESI.

A company may have control over documents based on a contractual relationship. For example, a duty to preserve documents may be imposed by contracts or contractual provisions in connection with:

- An agreement by the contracting parties to cooperate in litigation.
- A bankruptcy.
- A merger or acquisition.
- The creation or dismantling of a subsidiary.
- Employment severance agreements.

If a company determines that a third party over which it has control may have potentially responsive documents, it should issue a litigation hold notice to those third parties to ensure that they preserve the documents.

Securing Documents and ESI

As relevant documents and ESI are identified, they should be secured in a safe location. For example, a party may store relevant:

- Hard copy documents and back-up tapes:
  - in a locked room on-site accessible only to in-house counsel;
  - in an off-site storage facility; or
  - with outside counsel.
- Electronic documents belonging to individual custodians:
  - on the original hard drive, by swapping the custodian's hard drive for a new one;
  - on an imaged hard drive, which is an exact duplicate of the custodian's hard drive; or
  - on other appropriate **media**.
- ESI with its **cloud computing** provider.
- System files, including .PST or .NSF email files, on appropriate media in a safe, locked location.

The location of all preserved documents and information should be tracked in a log. Preserved information that remains on site at the company should be maintained in a locked room that is only accessible by a limited number of individuals in the company's legal department.

After the Pleadings are Filed

After the lawsuit is filed, counsel should confer with the client as soon as possible to discuss the location and preservation of potential evidence.

Discussions with the Client

Counsel and the client should communicate openly about discovery from the beginning of the case. Communication should be two-way, that is, both the client and counsel must share information freely so that the discovery process runs as smoothly and efficiently as possible and without surprises. Counsel and the client should have a general understanding of the documents and ESI that may be at issue in the case as early as possible so that they can make informed decisions about:

- The settlement value of the case.
- The likelihood of the case being dismissed.
- Whether to pursue alternative dispute resolution.
- How to proceed with discovery.

Counsel and the client should discuss the following topics as early as possible:

- Relevant discovery deadlines.
- Local rules and the court's preferences regarding a case management conference.
- Data sources and identify which:
  - have the data most relevant to the case;
  - have the highest volumes of relevant data;
  - are reasonably accessible; and
  - are not reasonably accessible.
- Staffing for data **collection** and review, including whether to use:

    - internal company staff;
    - outside counsel;
    - domestic contract attorneys; or
    - attorneys outside the US.
- What vendors to use, including:
    - the client's preferred vendors, if any;
    - realistic deadlines for document collection, review, and **production**;
    - the work to be performed by vendors; and
    - the preferred form of ESI.
- Estimates for the cost of reviewing and producing documents, considering variables such as:
    - data that is reasonably available in the company's ordinary course of business (such as active online data, near-line data, and offline storage and archives);
    - steps necessary to retrieve data that is not reasonably available in the company's ordinary course of business (such as back-up tapes and erased, fragmented, or damaged data); and
    - how to review the preserved data (for example, what technology to use, whether to review documents in-house or externally, and what document review platform to use).
- Sensitivities involved in producing documents and ESI, including:
    - communications protected by the attorney-client privilege;
    - items protected by the work-product doctrine;
    - documents or ESI that contain confidential health or personally-identifiable information of company employees or customers;
    - other applicable privileges or protections from disclosure, such as trade secrets; and
    - the need for a confidentiality agreement with opposing parties, or a protective order to prevent disclosure of sensitive information.

When is the Response to an RFP Due?

The producing party must generally respond to an RFP in writing within 30 days of service of the RFP. However, if a defendant was served with an RFP at the same time he was served with process and the initial pleading, then the defendant has 45 days from the date of service to respond. The court may order a longer or shorter period of time for response. (Fla. R. Civ. P. 1.350(b).)

Joint Stipulation for Extension of Time

The parties may agree to an extension of time regarding discovery responses. Attorneys usually agree to extensions without court action. These agreements are generally memorialized in a letter or email.

While informal agreements are the customary practice between attorneys, the best practice is for the counsel requesting additional time to prepare a joint stipulation, forward it to opposing counsel for his signature, file it with the court, and obtain a court order adopting the stipulation (Fla. R. Jud. Admin 2.505(d)).

If Opposing Counsel Does Not Agree to Extend Time

If the party propounding discovery will not agree to a reasonable extension of time to respond, counsel can file a motion for an extension of time. A motion for extension of time should:

- Demonstrate good cause for extending the time to respond to the discovery requests.
- Include a statement that the motion for additional time is not being made for delay.

Written Response Required from Producing Party

The producing party must respond to an RFP in writing by the due date (Fla. R. Civ. P. 1.350(b)). The producing party must include at least one of the following responses to each described item or category in the request:

- The inspection or production of responsive documents will be permitted as requested or copies of the documents provided as requested.
- That there is an objection to the requested time, place, or manner of production or inspection, and specify the grounds for the objection (Fla. R. Civ. P. 1.350(b)).
- That a privilege is being asserted for the document or item requested.

(Fla. R. Civ. P. 1.280(b)(6) and 1.350(b) .)

Objecting to Discovery Requests

Like any response, an objection must be in writing and must be served upon the requesting party. The objecting party must provide the following in the response if appropriate:

- The specific reason for the objection (Fla. R. Civ. P. 1.350(b)).
- Identification of the objectionable part of an item or category.
- If objecting to a requested form of ESI, a statement identifying the alternative form or forms of the ESI to be produced.

(Fla. R. Civ. P. 1.350(b).)

In Florida, parties may request discovery regarding any matter that is:

- Not privileged.
- Relevant to the subject matter of the pending litigation, including requests that relate to:
  - the claim or defense of the party seeking discovery or any other party; or
  - the existence, description, nature, custody, condition, and location of any books, documents, or other tangible things and the identity and location of persons having knowledge of any discoverable matter.

(Fla. R. Civ. P. 1.280(b)(1).)

For this reason, the responding party should object to requests that seek documents or information that are:

- Privileged.
- Irrelevant to the pending litigation.
- Not related to the claim or defense of any party.
- Overbroad.
- Vague or unclear, and lack sufficient specificity to enable a reasonable person to determine the information requested.
- Burdensome.
- Frivolous.
- Annoying, embarrassing, or oppressive.
- Unreasonably cumulative or duplicative.
- Obtainable from another source that is more convenient, less burdensome, or less expensive.
- Not reasonably calculated to lead to the discovery of admissible evidence (Fla. R. Civ. P. 1.280(b)(1)).

For additional information regarding the scope of discovery and RFPs, see Practice Note: Document Requests: Drafting and

Objections as to Time, Place, Manner, or Form
If the producing party objects to the requested time, place, or manner of production or inspection, the response should include a different reasonable time, place, or manner for complying with the request. If there is no reasonable time, place, manner, or form specified in the RFP for production or inspection, the producing party must indicate in its response a reasonable time, place, manner, and form of production or inspection which it intends to use. (Fla. R. Civ. P. 1.350(b).)

Specific Objections Regarding Electronically Stored Information
Under Rule 1.280(d) a party may object to discovery of ESI:

- From sources that are not reasonably accessible because of undue burden or cost (Fla. R. Civ. P. 1.280(d)(1)).
- Because the discovery sought is unreasonably cumulative or duplicative (Fla. R. Civ. P. 1.280(d)(2)).
- Because the discovery sought can be obtained from another source or in another manner that is:
  - more convenient;
  - less burdensome;
  - less expensive; or
  - the burden or expense of the discovery outweighs its likely benefit (Fla. R. Civ. P. 1.280(d)(2)).
- Because the burden or expense of the discovery outweighs its likely benefit, considering:
  - the needs of the case;
  - the amount in controversy;
  - the parties' resources;
  - the importance of the issues at stake in the action; and
  - the importance of the discovery in resolving the issues (Fla. R. Civ. P. 1.280(d)(2)).

Asserting Claims of Privilege
Documents or other requested information that are otherwise discoverable may be withheld based upon the following claims of privilege:

- Attorney-client privilege (§ 90.502, Fla. Stat.).
- Work-product doctrine (Fla. R. Civ. P. 1.280(b)(4)).

If a party claims that a discovery request calls for production of privileged materials that are "otherwise discoverable," the party should withhold the materials and in the response object to the request because it seeks privileged materials. The responding party should also produce with the response a separate privilege log that contains the following information:

- Information identifying the document without revealing the privileged information. When withholding a privileged letter for example, identify the sender, recipient, and date of the letter.
- Identify the nature of the privileged information with enough detail to allow the requesting party or judge to assess the applicability of the privilege, but without revealing the protected information.
- Identify the legal basis for the privilege (for example, attorney-client or work-product privilege)

(Fla. R. Civ. P. 1.280(b)(6).)

In Florida, until the trial court rules on the responding party's objections (usually in a hearing on the requesting party's

motion to compel), documents are not "otherwise discoverable" (Fla. R. Civ. P. 1.280(b)(6); see also *Gosman v. Luzinski*, 937 So. 2d 293, 296 (Fla. 4th DCA 2006)).

A party that fails to serve a privilege log does not necessarily automatically waive the privilege if the requests categorically sought privileged documents (*DLJ Mortg. Capital, Inc. v. Fox*, 112 So. 3d 644, 645-46 (Fla. 4th DCA 2013)).

Electronically Stored Information

Florida Rules of Civil Procedure 1.350(a) and 1.280(b)(3) permit discovery of ESI and allow the requesting party to specify the form in which the ESI is to be produced. If the request is for ESI, the producing party must either:

- Object to producing the ESI in the form the requesting party requests and state the form it intends to use.
- Produce the requested ESI in the form in which it was requested.
- Produce the requested ESI in a reasonably usable form or form in which it is ordinarily maintained if none is identified by the requesting party.

(Fla. R. Civ. P. 1.350(b).)

Florida Rule of Civil Procedure 1.200(a)(7) specifically encourages discussions and agreements from the parties regarding:

- The extent to which ESI should be preserved.
- The form in which ESI should be produced.
- Whether discovery of ESI should be conducted in phases or limited to particular individuals, time periods or sources.

(Fla. R. Civ. P. 1.200(a)(7).)

Forms of ESI

Common forms of ESI include:

- **Native files**.
- **PDFs**.
- **TIFFs** and **load files**.
- **Metadata**.

Native Files

A native file is an electronic document stored in the form in which it was created. In e-discovery, if documents are produced in their native form, the original software application might be needed to view the document (for example, a document created by word processing software might only be viewable on a computer with that software).

Native files typically contain metadata and information, such as comments and formulas that may be hidden when converted to TIFF or PDF files. For this reason, document production of native file format documents is particularly useful for production of spreadsheets and presentations, such as Microsoft PowerPoint presentations.

Documents in their native format have lower processing costs than images, such as PDFs or TIFFs, because there is less processing needed (native files already are searchable and should have their metadata intact). However, document review of native files may be more time-consuming.

PDFs

PDF is an acronym for Portable Document Format. A PDF is a file format created by Adobe Systems Incorporated that represents documents independent of the hardware and software used to create and view the file. A PDF is designed to capture the entirety of a document, including any text and images contained in the document. PDFs may also contain features added by the creator of the document, such as hyperlinks. A PDF file is considered a static image and generally cannot be altered or manipulated.

TIFFs and Load Files

TIFF (also known as TIF) is an acronym for Tagged Image File Format. A TIFF is an electronic file copy of a paper document, which contains no embedded text, fonts, or graphics. TIFF images cannot be searched for text and they do not contain metadata. Files in TIFF format often end with a .tif extension. They can be single or multi-page. A TIFF file is essentially a picture of how a document looks. Examples of TIFF files include:

- Scanned documents.
- Received faxes.

Because TIFF files are unsearchable, in a document production, a request for TIFF files are often accompanied by a request for load files, which contain metadata as well as searchable text identified through **optical character recognition** (OCR) software.

TIFF images were historically used for document production. Today, PDF files are used more often than TIFF files in document productions because PDFs have greater functionality than TIFFs, and PDF files generally are searchable.

Metadata

Metadata is information, often hidden, that describes the history, tracking, or management of an electronic file, such as:

- File name or title.
- Location or path of storage.
- Size.
- Subject.
- Comments.
- Author.
- Persons who have reviewed or edited the file and who have permission to access it.
- Dates of creation and modification.
- Dates of most recent printing, access, and metadata modification.
- Total editing time.

Metadata may be created automatically by a computer system or manually by a user. Where copies of disclosed documents are provided in native format, some metadata is typically disclosed with each document.

Searching ESI for Responsive Information

The landscape of discovery continues to change due to technological advances. Instead of reviewing a few boxes of documents for responsive documents, a producing party today may have thousands of potentially responsive emails to review, in cases large and small. Paper documents, if not already existing in digital form, are often scanned and converted to searchable files such as PDFs. The task of reviewing voluminous emails and other electronic documents is daunting, both in terms of time and money, especially when the items will be reviewed manually. However, data filtering technologies are increasingly used in the discovery process to:

- Evaluate documents and ESI for responsiveness and privilege.
- Identify responsive items faster and more efficiently.
- Reduce the amount of material requiring attorney review (the slowest and most costly aspect of the document review process).

Prior to production, the producing party can run searches against collected documents and ESI to identify responsive items with data filtering technologies such as:

- Keyword searches.
- Concept searches.
- Predictive coding.

Keyword Searches

Keyword searches are the traditional ESI search method. Keyword searches are run by comparing a list of words or combinations of words to the universe of potentially-responsive documents. Typically, documents containing one or more of these words are collected and made available for attorney review in a **document review platform**.

The list of keywords should be broad enough to capture all relevant documents. If the list is under-inclusive, relevant documents might not be retrieved, in which case they will never be seen by counsel.

For a comprehensive search, counsel should include:

- Terms used by the document custodians.
- Terms similar to those used by document custodians.
- Abbreviations.
- Common misspellings.

Searches should not be so broad that the result includes almost all of the ESI collected. Counsel often run overbroad searches because of the risk that they otherwise may miss relevant documents, but searches with common or generic keywords yield a large amount of irrelevant material.

Counsel should consider narrowing generic keywords by combining them with other terms. For example, if counsel wants to search all documents relating to "John Smith," rather than searching the terms "John" and "Smith" separately, counsel can search the two names together (for example, as an exact phrase, or with a proximity search like "John w/2 Smith" which would identify documents with the words John and Smith appearing within two words of each other) as well as John Smith's email address or other information specific to John Smith.

Concept Searches

Instead of (or in addition to) performing keyword searches, the producing party can use different technology that enables counsel to search for broader concepts or ideas. **Concept searches** are typically run within the pool of potentially-responsive ESI with the assistance of an e-discovery service vendor.

Concept searches are broader than keyword searches. Concept searching uses intelligence to understand the context in which the terms are used (such as a theme or category) to determine whether a particular document is responsive. By using concepts instead of keywords, searches yield relevant documents that fit within the defined concepts so that exact term matches are not necessary.

For example, the concept "financial statement" may be searched. Using adaptive concept searching technology, emails containing the terms "financials" or "financial report" or even "f/s" may generate results even if there is not an exact match to the term "financial statement."

Identifying concepts to search is similar to keyword searching. Counsel should:

- Identify themes that are relevant to the case.
- Run searches with the same terminology used by the document custodians.

Concept search technology identifies documents as responsive if they contain words or terms that fall within the context of the concepts being searched, regardless of whether the words or terms are actually referenced in the document. Therefore, unlike keyword searches, there is no need to search similar terms or misspellings since a concept search minimizes the error resulting from narrow or unknown terms. On the other hand, a concept search might generate over-inclusive results.

Predictive Coding

Predictive coding (which is a form of, and sometimes referred to as, technology-assisted review (TAR) or computer-assisted review (CAR) is a document review technology that uses algorithms to sort through a pool of ESI to "learn" how to review and code the collected ESI.

The exact process varies depending on the predictive coding vendor, but typically begins with a pool of potential ESI that has been previously organized (often using other technology such as concept searching or keyword searching). Once the pool of ESI has been organized:

- An experienced attorney takes a random or targeted sample of documents from the ESI, and categorizes each document as desired, such as "relevant," "not relevant," or "privileged." This sample of documents is sometimes referred to as a "seed set."
- The initial seed set of sample documents, now categorized (or "coded") by the attorney, is fed into the vendor's software, which analyzes the attorney's criteria and generates algorithms to establish a search model for testing.
- The attorney tests this search model against the pool of ESI (or a sample of the ESI) and evaluates the results.
- The above steps are typically repeated over the course of several iterations, as the program refines the algorithms and the search model reaches a reasonably acceptable level of accuracy.
- Throughout the iterative process, the program eventually trains itself to predict the manner in which the attorney would code the documents, so that the program can be used to search the entire pool of ESI based on relevance and privilege, and thereby identify the documents accordingly.

Predictive coding programs often evaluate the responsiveness of a document by either indicating "yes" or "no," or by providing a score based on a confidence level. For example, the program would assign each document a score between 1 and 100, with 100 meaning that the program is 100% confident that the document is responsive.

Cooperation Between Parties Regarding Discovery

The Florida rules encourage the parties to cooperate regarding discovery and to make agreements and stipulations reasonably necessary for the efficient disposition of the case (Fla. R. Civ. P. 1.200(a)). If the parties cannot informally resolve issues regarding ESI or the procedures or parameters of discovery, a party can file a motion with the court to:

- Enter a case management order (Fla. R. Civ. P. 1.200(a)).
- Limit, schedule, order, or expedite discovery (Fla. R. Civ. P. 1.200(a)(4)).
- Make appropriate determinations and orders regarding:
  - the exchange of documents and ESI (Fla. R. Civ. P. 1.200(a)(5));
  - the authenticity of documents and ESI (Fla. R. Civ. P. 1.200(a)(5));
  - the need for advance rulings from the court regarding admissibility of documents and ESI (Fla. R. Civ. P. 1.200(a)(6));
  - the extent to which ESI should be preserved (Fla. R. Civ. P. 1.200(a)(7));
  - the form in which ESI should be produced (Fla. R. Civ. P. 1.200(a)(7)); and
  - whether discovery of ESI should be conducted in phases or limited to particular individuals, time periods, or sources (Fla. R. Civ. P. 1.200(a)(7)).

Florida attorneys are specifically prohibited by the Rules of Professional Conduct from "making a frivolous discovery request" or intentionally failing "to comply with a legally proper discovery request by opposing party" (FL ST BAR Rule 4-3.4).

Further, prior to filing a motion to compel discovery under Rule 1.380(a), the movant must include a certification that the movant, in good faith, has conferred or attempted to confer with the person or party failing to make discovery in an effort to secure the information or material without court action (Fla. R. Civ. P. 1.380(a)(2)).

Preparing to Discuss ESI

To thoughtfully and comprehensively address document and ESI discovery issues with an opposing party, counsel should be prepared to discuss, as applicable:

- The client's documents, including:
  - the key players and custodians;
  - the sources of ESI;
  - the volume of ESI;
  - the volume of hard copy documents;
  - the use of **social media**;
  - the use of back-up systems; and
  - whether the client has a document retention policy.
- The client's preservation efforts, including details about the litigation hold, if applicable.
- The client's policy on employees using their personal devices for work (a Bring Your Own Device (BYOD) policy).
- Document collection and review, including:
  - the client's relevant document custodians;
  - proposed search methodologies;
  - whether to use predictive coding; and
  - anticipated costs associated with the production of documents and ESI.
- Document production, including:
  - the volume of documents and ESI the client expects to produce;
  - whether to produce documents and ESI in phases;

    - the client's preferred **format for production** of ESI; and
    - the production of metadata.
- Whether a confidentiality agreement or a protective order is needed.
- How to improve efficiencies, including use of:
    - privilege logs;
    - stipulations on **authenticity**;
    - stipulations on admissibility; or
    - other stipulations.
- Requesting documents from non-parties.
- How to narrow the scope of documents and ESI for production.

Modifying the Scope of Documents and ESI for Review

The parties may agree to limit the number of documents produced by:

- Eliminating duplicate documents.
- Modifying the relevant time frame.
- Phasing production.

Eliminating Duplicate Documents

Due to the nature of electronic documents, a large number of duplicate documents may exist in the universe of potentially responsive material. For example, an email sent to several recipients may exist in each person's email account at least once. Similarly, identical email attachments may exist in each custodian's files.

The producing party can reduce the volume of documents for attorney review and production by eliminating these duplicate documents (a process called **de-duplication** or de-duping). Eliminating duplicate documents benefits counsel for the requesting party because they should receive documents earlier in discovery and the number of documents to review is reduced. De-duplication can be applied:

- **To exact duplicates**. In other words, documents that are exactly the same, and in the same format.
- **To near duplicates**. For example, a word-processing document and the same document in PDF form.
- **Vertically**. Applying de-duplication technology within each custodian's documents.
- **Horizontally**. Applying de-duplication technology across all custodians' documents. Some software has the capability of tracking the source of each duplicate if that information is needed.

Counsel for the requesting party should weigh in on whether de-duplication is appropriate and, if so, how it should be applied. For example, if counsel wants to know all of the documents that were in the file of a particular custodian, they may only agree to vertical de-duplication of exact duplicates.

Modifying the Relevant Time Frame

Counsel may reduce the volume of responsive documents by narrowing the relevant time period for production, especially if the initial request was overly broad.

Phasing Discovery

Florida Rule of Civil Procedure 1.200(a)(7) specifically encourages discussions and agreements from the parties regarding whether discovery of ESI should be conducted in phases or limited to particular individuals, time periods, or sources (Fla. R. Civ. P. 1.200(a)(7)).

In resolving discovery disputes involving ESI, Florida courts will not allow overly broad requests, "fishing expeditions," or "unfettered access" to the opposing party's computers or records (see, for example, *Holland v. Barfield*, 35 So. 3d 953, 954 (Fla. 5th DCA 2010) and *Menke v. Broward Cty. Sch. Bd.*, 916 So. 2d 8, 12 (Fla. 4th DCA 2005)).

Duty to Supplement

In Florida, there is no duty to supplement a response to a request for discovery with after-acquired information if the party's response was complete when made (Fla. R. Civ. P. 1.280(f)). If counsel believes that responsive information has not been provided by the producing party, a motion to compel should be filed (Fla. R. Civ. P. 1.380(a)).

Costs of Production

Document production can be the largest litigation cost, both in large and small cases. Accordingly, all parties look to limit their respective costs relating to document production. Generally, the producing party bears the cost of discovery.

However, the Florida courts do not require one party to fund its adversary's litigation (*SPM Resorts, Inc. v. Diamond Resorts Mgmt., Inc.*, 65 So. 3d 146, 147 (Fla. 5th DCA 2011)). Trial courts have broad discretion in controlling and allocating discovery costs during the pendency of the case (*Katzman v. Rediron Fabrication, Inc.*, 76 So. 3d 1060, 1065 (Fla. 4th DCA 2011)). Some factors that may be taken into account by the court when allocating costs of discovery, particularly ESI, include the following:

- Needs of the case.
- Amount in controversy.
- Parties' resources.
- Importance of the issues at stake in the litigation.
- Importance of the proposed discovery in resolving the issues.

(Fla. R. Civ. P. 1.280(d)(2).)

Also, a responding party, instead of producing the documents by providing copies to the requesting party, may shift costs by making the documents available for inspection and/or copying (Fla. R. Civ. P. 1.350(b)).

Florida Rule of Civil Procedure 1.280(c) allows any party or person from whom discovery is sought to move for a protective order as a result of undue burden or expense (Fla. R. Civ. P. 1.280(c)). This applies to discovery of ESI from sources that the person or party identifies as not reasonably accessible because of burden or cost as well (Fla. R. Civ. P. 1.280(d)(1)).

If the producing party has objected to the production of ESI based upon undue burden or expense, the requesting party must then show "good cause" for the requested discovery request and, after a hearing, the Court may:

- Order the discovery from the sources or in the formats requested.
- Specify conditions of the discovery, including allocating costs and expenses for the discovery to be paid by the party seeking the discovery.

(Fla. R. Civ. P. 1.280(d)(1).)

After any hearing on a motion to compel discovery, the court shall require the party whose conduct necessitated the motion to pay the moving party its reasonable expenses, which may include attorney's fees, unless:

- Movant failed to certify in its motion that a good faith effort was made to obtain the discovery without court intervention.
- The opposition to the motion was substantially justified.
- Other circumstances make an award of expenses unjust.

(Fla. R. Civ. P. 1.380(a)(4).)

Counsel should note, however, that if her client obtains a judgment in the litigation, it will be generally entitled to recover taxable costs incurred in discovery (§ 57.041, Fla. Stat.). Florida courts have specifically upheld a trial judge's discretion in taxing the costs of the copies obtained during discovery (*Mitchell v. Osceola Farms Co.*, 574 So. 2d 1162, 1163 (Fla. 4th DCA 1991)). The prevailing party must file a motion under Florida Rule of Civil Procedure 1.525 to recover costs (and attorney's fees, if applicable) within 30 days of the filing of judgment, even if the judgment expressly includes a finding that the party is entitled to such items (*Parrot Cove Marina, LLC v. Duncan Seawall Dock & Boatlift, Inc.*, 978 So. 2d 811, 816 (Fla. 2d DCA 2008)).

Privilege Log (FL)

A sample privilege log that may be used during discovery in Florida civil litigation to list certain documents and other materials that counsel is withholding from production on grounds of attorney-client privilege, work product protection, or another recognized privilege or protection. This Standard Document has integrated drafting notes with important explanations and drafting tips.

IN THE CIRCUIT COURT OF THE [NUMBER] JUDICIAL CIRCUIT
IN AND FOR [COUNTY NAME] COUNTY, FLORIDA

[NAME],
Plaintiff[s],
vs.
[NAME],
Defendant[s].
_____/

Case No. [NUMBER]

[PLAINTIFF/DEFENDANT [PARTY NAME]]'S PRIVILEGE LOG

Date	Doc Type	No. of Pages	Authors	Recipients	Persons Copied	Description	Privilege or Protection Asserted

Dated:[[MONTH] [DAY], [YEAR]]

Respectfully submitted,

[NAME OF LAW FIRM]

F

[STREET ADDRESS]

[CITY], FL [ZIP CODE]

[TELEPHONE NUMBER]

[FAX NUMBER]

BY_____

[NAME OF ATTORNEY]

Florida State Bar No. [NUMBER]

[EMAIL ADDRESS]

Attorney for [Plaintiff(s)/Defendant(s) [PARTY'S NAME]]

CERTIFICATE OF SERVICE

I hereby certify that this [motion/notice/brief/[OTHER DOCUMENT]] was served via [the Florida Court E-Filing Portal/email/U.S. mail/fax/hand-delivery] on [DATE] upon: [COUNSEL'S NAME(S)], counsel for [PARTY'S NAME], at [[FIRM NAME], [MAILING ADDRESS], and [EMAIL ADDRESSES]].

/s [ATTORNEY'S NAME]

[ATTORNEY'S NAME]

Discovery Deficiency Letter (FL)

A sample discovery deficiency letter outlining deficiencies in a production by an opposing party and requesting additional discovery materials to remedy these deficiencies. This Standard Document has integrated notes with important explanations and drafting tips, including discussion on the purpose of a discovery deficiency letter, meet and confer requirements, and substantive tips on drafting the letter.

[LAW FIRM LETTERHEAD]

By: [DELIVERY METHOD]

[ADDRESS LINE 1]

[ADDRESS LINE 2]

[ADDRESS LINE 3]

Re: [STYLE OF CASE], Case No. [CASE NUMBER]]

Dear [OPPOSING COUNSEL]:

I have received [plaintiff [NAME]/defendant [NAME]/your client [NAME]]'s responses to [FULL TITLE OF DISCOVERY REQUEST] in the above-referenced matter.

[The responses received to date are deficient in material ways/The objections raised to the discovery requests concerning [SUBJECT] are without merit/The privileges claimed are without merit] [and additional responses are required to remedy these deficiencies].

This letter is an attempt to resolve these [deficiencies/discovery disputes] without court intervention and avoid a motion to compel [and for sanctions] under Florida Rule of Civil Procedure 1.380(a). To that end, I respectfully request that [we discuss these issues/you satisfy your obligations by providing the requested information] promptly.

Specifically, I note the following deficiencies:

- In response to [document request/interrogatory/request to admit] number [NUMBER], [EXPLANATION OF DEFICIENCY].
- Please provide [EXPLANATION OF WHAT INFORMATION IS NEEDED FOR A COMPLETE RESPONSE].
- [ADDITIONAL DEFICIENCIES.]

Because the requested discovery is essential to this litigation, I ask that [we speak/you provide a response to this letter/you provide the requested information] on or before [DATE]. If I do not hear from you by [DATE], I intend to file a motion with the court to compel [responses/production/answers/designation of a corporate witness,][and for sanctions,] under Florida Rule of Civil Procedure 1.380(a).

If any aspect of this letter requires clarification, please contact me as soon as possible. Thank you in advance for your cooperation.

Sincerely,

_____

[ATTORNEY'S NAME]

Interrogatories: Responding to Interrogatories

This Practice Note addresses responding to interrogatories under ***Rule 33 of the Federal Rules of Civil Procedure*** *(FRCP). Specifically, this Note addresses the ways in which a party may respond to interrogatories, including answering and objecting to interrogatories, as well as the requirements for serving a proper response to interrogatories. This Note also discusses key timing issues for counsel when responding to interrogatories.*

Contents

H

Timing of Response to Interrogatories
30 Days to Respond in General
Requesting an Extension
Serving Responses
Supplementing or Amending Answers

In federal civil litigation, **interrogatories** are written questions that a party generally must answer under oath. A party to a federal civil lawsuit uses interrogatories to obtain information in **discovery** from another party in the lawsuit. Federal Rule of Civil Procedure (FRCP) 33 governs interrogatories in federal civil litigation.

When a party receives properly served interrogatories under FRCP 33, the party typically has a limited time to respond, and its response must comply with FRCP 33's specific requirements. To avoid the risk of motion practice and potential sanctions, the responding party must timely serve proper answers or objections to interrogatories.

This Note addresses FRCP 33's requirements and provides guidance to counsel on how to prepare and serve proper answers and objections to interrogatories.

Ways to Respond to Interrogatories

Generally, a party may respond to interrogatories by:

- Providing written answers to the interrogatories (see Answering Interrogatories).
- Referring to and producing responsive documents or **electronically stored information** (ESI) (see Option to Produce Business Records).
- Objecting to the interrogatories (see Objecting to Interrogatories).
- Objecting to some interrogatories and responding to others by:
  - providing written answers; or
  - opting to produce responsive business records or ESI.
- Objecting to portions of interrogatories but also, subject to the asserted objections, responding by:
  - providing written answers; or
  - opting to produce business records or ESI.

- Requesting an extension of time to respond to some or all of the interrogatories (see Requesting an Extension).

(FRCP 33(b)(3), (4); FRCP 33(d).)

Who Must Answer Interrogatories

Absent objections, each interrogatory must be separately answered by:

- The party to whom the interrogatories are directed, if the party is an individual.
- A designated officer or agent, if the responding party is an entity (corporation, partnership, association or governmental agency).

(FRCP 33(b)(1), (3).)

In practice, counsel usually prepare answers to interrogatories for their client's review and signature (see Preparing Responses to Interrogatories).

Interrogatories to Individuals

If interrogatories are directed to an individual party, that individual must provide and sign any answers under oath (FRCP 33(b)(1), FRCP 33(b)(3), FRCP 33(b)(5); see also The "Under Oath" Requirement and The Client's Signature).

Interrogatories to Entities

If interrogatories are directed to an entity, FRCP 33 requires the entity to designate "any" officer or agent to answer any non-objectionable interrogatories and sign the answers under oath on the entity's behalf (FRCP 33(b)(1)(B), FRCP 33(b)(5)). The responding entity generally has the discretion to choose the representative to answer the interrogatories on its behalf (see *Rhodes v. Elec. Data Sys. Corp.*, 2007 WL 840307, at *1 (E.D. Cal. Mar. 19, 2007), report and recommendation adopted, 2007 WL 1241847 (E.D. Cal. Apr. 27, 2007)). The person designated to answer interrogatories on an entity's behalf does not need personal knowledge of the information used to answer the interrogatories (*Jiminez-Carillo v. Autopart Int'l, Inc.*, 285 F.R.D. 668, 669 (S.D. Fla. 2012)). However, the representative must gather and disclose all responsive information available to the entity (FRCP 33(b)(1)(B); Entity's Duty to Conduct Reasonable Inquiry).

Answering Interrogatories

Generally, to the extent a party does not object to an interrogatory, the party must answer each interrogatory:

- In writing (see Provide Written Answers That Conform to Local Rules).
- Separately (see Provide Separate Answers).
- Fully (see Provide Complete Answers).
- Under oath (see The "Under Oath" Requirement).

(FRCP 33(b)(3).)

The failure to answer (in whole or in part) or properly object to interrogatories may result in motion practice and sanctions (FRCP 26(g); FRCP 37(a)(3)(iii); FRCP 37(d); and see Practice Note, Sanctions in Federal Court: Sanctions for Improper Disclosures or Written Discovery Under FRCP 26(g) and Sanctions for Failure to Make Required Disclosures or Cooperate in Discovery Under FRCP 37).

Provide Written Answers That Conform to Local Rules

Before drafting answers to interrogatories, counsel should consult the district court's local rules. Many district courts impose specific requirements for drafting answers and objections to interrogatories, such as including the text of the original interrogatory before each answer or objection.

Provide Separate Answers

A party must separately respond to each interrogatory (FRCP 33(b)(3)). Generally, counsel should answer or object to each interrogatory in a numbered paragraph that corresponds to the number of the interrogatory as served. Counsel should repeat a response even if it is the same for two or more interrogatories.

Provide Complete Answers

FRCP 33(b)(3) requires a party to fully answer an interrogatory using non-privileged information that:

- Is immediately available to the party, or to the party's attorneys, agents, or representatives.
- Is under its control.
- Can be obtained after reasonable investigation.

(*Younes v. 7-Eleven, Inc.*, 2015 WL 8543639, at *12-13 (D.N.J. Dec. 11, 2015); *Malibu Media, LLC v. Tashiro*, 2015 WL 2371597, at *22 (S.D. Ind. May 18, 2015), report and recommendation adopted, 2015 WL 3649359 (S.D. Ind. June 11, 2015); *Baker v. Cnty. of Missaukee*, 2013 WL 5786899, at *3 (W.D. Mich. Oct. 28, 2013); *Nat'l Fire Ins. Co. of Hartford v. Jose Trucking Corp.*, 264 F.R.D. 233, 238-39 (W.D.N.C. 2010).)

If the responding party cannot fully answer an interrogatory because it is still in the process of gathering information or expects to receive responsive information after the response is due, the party should state that in its response and supplement or amend its answers as soon as possible (see Supplementing or Amending Answers). A party who is unable to answer an interrogatory after reasonable investigation must describe in its answers the efforts taken to obtain the information (see *Bryant v. Armstrong*, 285 F.R.D. 596, 612 (S.D. Cal. 2012); *Zanowic v. Reno*, 2000 WL 1376251, at *6 n.1 (S.D.N.Y. Sept. 25, 2000)).

In addition to a party's obligation to conduct a reasonable investigation, FRCP 26(g) imposes a separate obligation on counsel to conduct a reasonable inquiry when preparing and signing interrogatory responses into the factual basis of the responses and to ensure that their client has provided all responsive information (see Counsel's Duty to Conduct Reasonable Inquiry).

Counsel typically assert at least partial objections to some, if not all, interrogatories. However, to avoid the time and expense of litigating a motion to compel and possible sanctions, the best practice is to answer each interrogatory as fully as possible within the time the answers are due, while preserving any necessary objections. If only part of an interrogatory is

objectionable, a party should answer the remaining, non-objectionable portion (see Objecting to Interrogatories).

The "Under Oath" Requirement

A responding party must attest under oath to the truth and accuracy of (**verify**) its answers to interrogatories (FRCP 33(b)(3)). A responding party generally satisfies the under oath requirement by signing and attaching a separate verification page after its written responses, in the form of either:

- A sworn statement that the party signs and has notarized. For example, a model verification for an individual signing in the US may state:
    - "I, [RESPONDING PARTY], have read [ASKING PARTY]'s [NUMBER] Set of Interrogatories and my answers to those interrogatories, which are true to the best of my knowledge, information, and belief. I declare under penalty of perjury that the foregoing is true and correct."
- A declaration under 28 U.S.C. § 1746 that the party signs, which does not require notarization. For example, a model verification for a corporate representative signing in the US may state:
- "I, [CORPORATE REPRESENTATIVE], am [TITLE] of [CORPORATE PARTY]. I am the agent of [CORPORATE PARTY] for the purpose of answering [ASKING PARTY]'s [NUMBER] Set of Interrogatories. I have read the foregoing interrogatories and the answers to those interrogatories, which are true according to the best of my knowledge, information, and belief. I declare under penalty of perjury that the foregoing is true and correct."

If the individual or designated representative who executes the interrogatory answers is located outside the United States, additional language in the verification is necessary (28 U.S.C. § 1746(1)).

Verification on Information and Belief

In many courts, individual verifications based in part on information and belief generally satisfy the "under oath" requirement in FRCP 33 (for example, 28 U.S.C. § 1746(2); *Zanowic*, 2000 WL 1376251, at *5; *State Farm Mut. Auto. Ins. Co. v. Lincow*, 2008 WL 697252, at *5 (E.D. Pa. Mar. 10, 2008); and see *Lackey v. SDT Waste & Debris Servs.*, 2013 WL 5772325, at *5-6 (E.D. La. Oct. 23, 2013)). However, some courts require individual parties to verify the truth and accuracy of answers solely on the basis of personal knowledge. These courts have concluded that it is improper for an individual party to verify answers even in part upon information and belief (see, for example, *U.S. ex rel. O'Connell v. Chapman Univ.*, 245 F.R.D. 646, 650 (C.D. Cal. 2007); *Nagler v. Admiral Corp.*, 167 F.Supp 413, 415 (S.D.N.Y. 1958)).

In contrast, a designated corporate representative generally does not need personal knowledge of the responsive information disclosed in an entity's answers to interrogatories (*De la Torre v. Lockheed Martin Corp.*, 2014 WL 2931268, at *12 (D.N.J. June 30, 2014); *Jiminez-Carillo*, 285 F.R.D. at 669). Particularly in large entities, the designated representative rarely has first-hand personal knowledge of all of the information needed to answer interrogatories. In these cases, the designated representative must gather all responsive information available to the company, such as through discussions with other employees or review of company records and books, and verify the answers upon information and belief (FRCP 33(b)(1)(B); *eBay, Inc. v. Digital Point Sols., Inc.*, 2010 WL 147967, at *5 (N.D. Cal. Jan. 12, 2010); *Shepherd v. ABC, Inc.*, 62 F.3d 1469, 1482 (D.C. Cir. 1995); *Casson Const. Co. v. Armco Steel Corp.*, 91 F.R.D. 376, 382 (D. Kan. 1980); *In re Folding Carton Antitrust Litig.*, 76 F.R.D. 417, 419 (N.D. Ill. 1977)).

Verification by Counsel

Entities may designate in-house counsel to draft and verify answers to interrogatories. However, outside counsel who prepared the interrogatories generally may not verify the answers in place of their client (see, for example, *Villareal v. El Chile, Inc.*, 266 F.R.D. 207, 211 (N.D. Ill. 2010); but see *Shire Labs., Inc. v. Barr Labs., Inc.*, 236 F.R.D. 225, 227 (S.D.N.Y. 2006)).

Option to Produce Business Records

FRCP 33 gives parties the option to produce business records in lieu of providing a written answer to an interrogatory if both:

- The answer to the interrogatory can be determined by examining, auditing, compiling, abstracting, or summarizing a party's business records (including ESI).
- The burden of obtaining the answer from those records will be substantially the same for either party. Courts evaluate this burden by looking at:
  - the responding party's familiarity with its own documents;
  - the cost of necessary research to locate responsive information among records; and
  - the nature of the records.

(FRCP 33(d); *United States v. Kellogg Brown & Root Servs., Inc.*, 284 F.R.D. 22, 30 (D.D.C. 2012); *Taube Corp. v. Marine Midland Mortg. Corp.*, 136 F.R.D. 449, 454 (W.D.N.C. 1991).)

If opting to produce business records in response to interrogatories, the responding party must, for each answer:

- Affirmatively state its election to produce business records in lieu of providing a written answer.
- Specify the responsive records in sufficient detail to allow the asking party to locate and identify the records as readily as the responding party.
- Provide an index to guide the asking party to the responsive documents, if producing voluminous documents.
- Give the asking party a reasonable opportunity to examine and make copies, compilations, abstracts, or summaries of the records.

(FRCP 33(d)(1), (2); *Graske v. Auto-Owners Ins. Co.*, 647 F. Supp. 2d 1105, 1108-09 (D. Neb. 2009); *Walt Disney Co. v. DeFabiis*, 168 F.R.D. 281, 284 (C.D. Cal. 1996); *O'Connor v. Boeing N. Am., Inc.*, 185 F.R.D. 272, 278 (C.D. Cal. 1999).)

FRCP 33(d) cannot be used to send the asking party on a fishing expedition or to avoid answering an interrogatory. The responding party may only refer to records if it knows the records contain information responsive to the interrogatory. Moreover, simply referring to a mass of documents in response to an interrogatory is insufficient (see *Mullins v. Prudential Ins. Co. of Am.*, 267 F.R.D. 504, 514-15 (W.D. Ky. 2010); *Pulsecard, Inc. v. Discover Card Servs., Inc.*, 168 F.R.D. 295, 304-305 (D. Kan. 1996); *Sabel v. Mead Johnson & Co.*, 110 F.R.D. 553, 555 (D. Mass. 1986)).

Because records must be offered in a manner that permits the same direct and economical access available to the responding party, the responding party may be required to produce previously made summaries or compilations of the responsive records (*United States ex rel. Englund v. Los Angeles Cnty.*, 235 F.R.D. 675, 680 (E.D. Cal. 2006)).

Preparing Responses to Interrogatories

Counsel typically prepares written answers interrogatories after communicating with the client to collect responsive information. Where the responding party is an entity, counsel generally communicates with the designated representative (or, in some cases, another representative of the entity who is counsel's point of contact) to determine what information to include in the answers. For more on the obligations of counsel and parties in answering interrogatories, see Counsel's Duty to Conduct Reasonable Inquiry and Entity's Duty to Conduct Reasonable Inquiry.

Once counsel prepares the answers, the individual verifying them must carefully review the answers to ensure their accuracy. After the draft is finalized, the party (or if the party is an entity, the designated representative) must verify under oath that the answers are true and accurate. The verification usually appears on a separate page that is attached to the answers. The party or designated representative must sign the verification, and counsel must also sign the response, as with any other discovery paper (FRCP 26(g)). (See The "Under Oath" Requirement and Signing Answers and Objections to Interrogatories.)

A party may object to an interrogatory in lieu of providing a written answer (FRCP 33(b)(3)). Counsel for the responding party typically determines which interrogatories are objectionable and prepares written objections to them (see Objecting to Interrogatories).

Use of Answers to Interrogatories

When drafting answers to interrogatories, counsel should keep in mind that litigants can use answers to interrogatories:

- As the Federal Rules of Evidence permit, including:
  - for impeachment where interrogatory responses are inconsistent with other testimony; and
  - as admissions against interest which the court can admit into evidence at trial.
- In pre-trial motions, including motions to dismiss and motions for **summary judgment**.
- During **mediation** or settlement negotiations.

(FRCP 33(c); *Brown v. White's Ferry, Inc.*, 280 F.R.D. 238, 243 (D. Md. 2012); *Jackson-Hall v. Moss Point Sch. Dist.*, 2012 WL 1098524, at *4 (S.D. Miss. Apr. 2, 2012).)

Reasonable Inquiry Requirement

When answering interrogatories, counsel and parties are obligated to conduct a reasonable inquiry to ensure that answers to non-objectionable interrogatories reflect all available (or reasonably ascertainable) non-privileged and responsive information.

Individual's Duty to Conduct Reasonable Inquiry

An individual party has a duty to reasonably investigate whether his responses to an opposing party's interrogatories are complete and accurate. The failure to take reasonable steps to ensure that answers are complete and accurate may lead to sanctions against the party under FRCP 26(g), FRCP 37, or a court's inherent authority (see, for example, *Rodman v. Safeway Inc.*, 2016 WL 5791210, at *3-5 (N.D. Cal. Oct. 4, 2016) (sanctions under FRCP 26(g); *Malibu Media, LLC v. Tashiro*, 2015 WL 2371597, at *22-38 (S.D. Ind. May 18, 2015) (recommending sanctions under the court's inherent authority), report and recommendation adopted, 2015 WL 3649359 (S.D. Ind. June 11, 2015); *State Farm Mut. Auto. Ins. Co. v. New Horizont, Inc.*, 250 F.R.D. 203, 219-23 (E.D. Pa. 2008) (granting sanctions under FRCP 37)). For more on available sanctions against a party, see Practice Note, Sanctions in Federal Litigation.

Organization's Duty to Conduct Reasonable Inquiry

An entity must answer interrogatories if it can obtain the responsive information from its employees, agents, or other persons who acted on the entity's behalf. Therefore, counsel must ensure that the representative designated to answer interrogatories

provides all available responsive information in the entity's possession or control, and not just information that may be within the personal knowledge of that individual (FRCP 33(b)(1)(B)).

An entity generally satisfies its duty to obtain responsive information by:

- Making reasonable inquiries of its employees, agents, and persons under the entity's control.
- Conducting a reasonable search of its business records.

(*Morris v. Lowe's Home Ctrs., Inc.*, 2012 WL 5347826, at *4-5 (M.D.N.C. Oct. 26, 2012).) This duty typically falls on the designated representative, as interviewing employees and reviewing business records to gather information also form a basis for verifying the answers (see *Shepherd v. Am. Broad. Cos., Inc.*, 62 F.3d 1469, 1482 (D.C. Cir. 1995); see also Verification on Information and Belief).

Counsel's Duty to Conduct Reasonable Inquiry

FRCP 26(g) imposes an obligation on the attorney who signs responses to interrogatories to both:

- Make a reasonable effort to ensure that a client has provided all available responsive information in the responses.
- Conduct a reasonable inquiry into the factual basis of the responses.

(*Heller v. City of Dallas*, 303 F.R.D. 466, 476 (N.D. Tex. 2014); *Morris*, 2012 WL 5347826, at *4).)

This duty arises from the certification an attorney makes under FRCP 26(g) when signing responses (FRCP 26(g)(1); and see Significance of Counsel's Signature).

A court determines whether the signing attorney's inquiry was objectively reasonable on a case-by-case basis, and at the time the responses were served. Relevant factors include:

- The complexity of the issues in the case.
- The availability of witnesses or documents.
- The past working relationships between the attorney and the client.
- The time available to conduct an investigation.

(See *S2 Automation LLC v. Micron Tech., Inc.*, 2012 WL 3656454, at *31 (D.N.M. Aug. 9, 2012); *Morris*, 2012 WL 5347826, at *4-5.)

Counsel's failure to adhere to this duty may result in sanctions under FRCP 26(g) or other sources of authority for sanctions

Objecting to Interrogatories

FRCP 33 expressly permits counsel to assert valid objections to an interrogatory instead of answering the interrogatory. Counsel must:

- Specifically state the objection (see Specific Objections).
- Timely assert the objection with any answers to the interrogatories (see Timing of Response to Interrogatories).

(FRCP 33(b)(2), (4).)

If a party fails to object within the deadline for responding, the party likely waives the objection (FRCP 33(b)(4); *Nat'l Fire Ins. Co. of Hartford v. Jose Trucking Corp.*, 264 F.R.D. 233, 238 (W.D.N.C. 2010)). However, a court has the discretion to excuse a waiver of objections for good cause (see, for example, *Cheshire v. Air Methods Corp.*, 2015 WL 7736649, at *3 (W.D. La. Nov. 30, 2015)).

If only part of an interrogatory is objectionable, counsel should:

- State the objection.
- Specify the objectionable portion.
- Answer the non-objectionable portion.

(See 1993 Advisory Committee Note to FRCP 33(b)(2).)

A district court's local rules also may make this a requirement (see, for example, S.D. Fla. L. Civ. R. 26.1(e)(1) ("no part of an interrogatory shall be left unanswered merely because an objection is interposed to another part of the interrogatory")).

Specific Objections

FRCP 33(b)(4) requires counsel to state any objections with specificity. In practice, counsel almost always assert objections in response to interrogatories. Although it is important to preserve all necessary objections, counsel should remember that objections asserted solely for any improper purpose, such as to delay or needlessly increase the cost of litigation, may result in sanctions (FRCP 26(g); and see Significance of Counsel's Signature).

Common objections include that the interrogatory:

- Seeks information that is not relevant to the parties' claims or defenses. Given the December 1, 2015 amendments to the FRCP, a court is likely to overrule as improper an objection that an interrogatory is "not relevant to the subject matter of the case" or "not reasonably calculated to lead to the discovery of admissible evidence." For more information, see Article, The FRCP Amendments: Small Step or Giant Leap?: Narrowed Scope of Discoverable Information: Relevant to a Claim or Defense.
- Seeks information that is not proportional to the needs of the case under FRCP 26(b)(1) (see 2015 Advisory Committee Notes to FRCP 33). When analyzing potential objections, counsel should consider the proportionality factors under FRCP 26(b)(1), which limits the scope of discovery based on:
  - the importance of the issues at stake in the case;
  - the amount in controversy;
  - the parties' relative access to relevant information;
  - the parties' resources;
  - the importance of the discovery in resolving the case; and
  - whether the burden or expense of the discovery outweighs its likely benefit.
- Calls for opinions and conclusions of pure law.
- Is too burdensome to answer. For example, a court may find an interrogatory too burdensome if it requires the responding party to perform extensive research or investigation to acquire the requested information.
- Is overbroad.
- Seeks information that is cumulative or duplicative.
- Seeks information that can be obtained from a more convenient, less burdensome, or less expensive source.
- Is vague and ambiguous.
- Calls for privileged, confidential or **trade secret** information. (For more information about the **attorney-client privilege** and **work product doctrine**, see the Attorney-Client Privilege and Work Product Doctrine Toolkit. For more information on trade secrets, see Practice Note, Protection of Employers' Trade Secrets and Confidential Information.)
- Is premature. For example, some courts do not permit parties to serve contention interrogatories until other discovery

has concluded (see Practice Note, Interrogatories: Initial Considerations: Opinion or Contention Interrogatories). However, counsel should be aware that some courts do not view prematurity as a valid objection (see, for example, *Remy Inc. v. Tecnomatic, S.P.A.*, 2013 WL 1183334, at *1 (S.D. Ind. Mar. 21, 2013)).

- Exceeds the number of permissible interrogatories allowed by FRCP 33, a court order, or the parties' stipulation. (For more information on the permissible number of interrogatories a party may serve, see Practice Note, Interrogatories: Initial Considerations: Number of Interrogatories.)

(See, for example, *State Farm Fire & Cas. Co. v. Gates, Shields & Ferguson, P.A.*, 2015 WL 8492030, at *2 (D. Kan. Dec. 10, 2015) (applying amended FRCP and sustaining irrelevancy objections to interrogatories); *Shoemake v. McCormick, Summers & Talarico II, LLC*, 2011 WL 5553652, at *4-5 (D. Kan. Nov. 15, 2011) (discussing objections to relevancy); *L.H. v. Schwarzenegger*, 2007 WL 2781132, at *2 (E.D. Cal. Sept. 21, 2007) (objections as overly burdensome); *George K. Baum Advisors LLC v. Sprint Spectrum, L.P.*, 2013 WL 5255019, at *4 (D. Kan. Sept. 17, 2013) (objections based on improper legal conclusions).)

General Objections and Boilerplate Language

In some circumstances, counsel may need to make objections to some aspect of the interrogatories that apply to all of the interrogatories and any answers to them, such as objections to:

- Burdensome or otherwise unreasonable instructions.
- Improper definitions of a party or other terms.
- The applicable time period stated in the interrogatories.
- Interrogatories in excess of the 25-interrogatory limit or another limit agreed to by the parties or that the court orders.
- Interrogatories that are untimely served, such that a response is due after the discovery cut-off date.

Counsel typically may assert these kinds of objections in a section called "General Objections" before responding to specific interrogatories. If including a "General Objections" section, counsel should articulate a specific basis (and, if applicable, supporting facts) for each general objection.

In practice, interrogatory responses often include boilerplate objections in the "General Objections" section that do not articulate a specific basis for each of the general objections, along with a statement that the objections apply to the entire set of interrogatories and are incorporated into each specific response to the interrogatories. However, in part because FRCP 33 requires objections to be specific, many courts conclude that this practice violates the FRCP. Courts may disregard or strike general, boilerplate objections or even impose sanctions (see, for example, *Heller*, 303 F.R.D. 466 at 483-84); *Vidal v. Metro-N. Commuter R.R. Co.*, 2013 WL 1310504, at *1 (D. Conn. Mar. 28, 2013); *Chavez v. Mercantil Commercebank, N.A.*, 2011 WL 1135005, at *2 (S.D. Fla. Mar. 28, 2011); *Kansas Heart Hosp., L.L.C. v. Exec. Risk Indem., Inc.*, 2007 WL 1125772, at *2 (D. Kan. Apr. 16, 2007); see also *Liguria Foods, Inc. v. Griffith Labs., Inc.*, 2017 WL 976626 (N.D. Iowa Mar. 13, 2017) (discussing at length the perils of boilerplate objections and admonishing counsel)).

Courts have also found that providing answers to specific interrogatories "subject to and without waiving" objections, a boilerplate phrase commonly used in practice, does not comply with the FRCP (see, for example, *Liguria Foods, Inc.*, 2017 WL 976626, at *11-12, *16 n.17; *Heller*, 303 F.R.D. at 487).

Counsel should avoid making these types of boilerplate objections in response to interrogatories. For a sample response to interrogatories that complies with the FRCP, see Standard Document, Interrogatories: Response to Interrogatories (Federal).

Signing Answers and Objections to Interrogatories

As with other discovery papers, counsel must sign a party's response to interrogatories under FRCP 26(g). FRCP 33 also

imposes signature requirements on counsel and the responding party.

The Client's Signature

FRCP 33(b)(5) requires the person who answers interrogatories to sign the answers. A party (or, if the party is an entity, its designated representative) satisfies this requirement by verifying the answers and signing the verification, which is then attached to the response (see The "Under Oath" Requirement).

If all of the interrogatories are wholly objectionable and no answers are provided, only the attorney who prepared the objections, and not the responding party, needs to sign the objections (see Counsel's Signature). The responding party does not need to provide a verification until the parties (with our without court intervention) resolve the objections and the responding party provides answers.

Counsel's Signature

FRCP 26 requires at least one attorney of record to sign every discovery request, response, or objection (FRCP 26(g)(1)). FRCP 33(b)(5) separately requires the attorney who objects to interrogatories to sign the objections. In practice, this means that counsel who prepared a response containing objections should sign it (as with any other discovery pleading) and, if answers have also been provided, attach the signed verification of the party (or, if the party is an entity, its designated representative) (see The "Under Oath" Requirement).

Significance of Counsel's Signature

By signing interrogatory responses, an attorney certifies that, to the best of her knowledge, information, and belief formed after a reasonable inquiry, answers or objections to the interrogatories are:

- Consistent with the FRCP's requirements.
- Warranted by existing law or by a non-frivolous argument for extending, modifying, or reversing existing law, or for establishing new law.
- Not interposed for any improper purpose, such as to:
  - harass;
  - cause unnecessary delay; or
  - needlessly increase the cost of litigation.
- Neither unreasonable nor unduly burdensome or expensive, considering:
  - the needs of the case;
  - prior discovery in the case;
  - the amount in controversy; and
  - the importance of the issues at stake in the action.

(FRCP 26(g)(1)(B)(i)-(iii).)

A court may sanction an attorney who signs and serves responses to interrogatories that violate one of FRCP 26(g)(1)(B)'s provisions at the time the interrogatories are served

Timing of Response to Interrogatories

30 Days to Respond in General

FRCP 33 requires a responding party to answer or object to interrogatories within 30 days after service of the interrogatories, unless:

- The parties stipulate to a longer or shorter time to respond.
- The court orders a shorter or longer time to respond.

(FRCP 33(b)(2).)

A party also may have additional time to respond based on other factors, such as the method the asking party used to serve the interrogatories

If a party fails to object within the applicable deadline, the party may waive all objections (see Objecting to Interrogatories).

Requesting an Extension

If counsel needs more time to serve responses to interrogatories, counsel should request an extension before the expiration of the initial deadline. Similarly, if counsel has already obtained an extension but requires additional time to respond, counsel should request the subsequent extension before the expiration of the stipulated period.

Counsel generally may stipulate to extend the time for responding to interrogatories without court approval, unless the extension would interfere with the time set for completing discovery, a hearing on a motion, or trial (FRCP 29(b)). However, counsel should check the local and judge's rules, which may limit the number of times parties may stipulate to an extension or contain other requirements for stipulations to extend the response deadline.

If opposing counsel does not agree to the extension, or court approval for the extension is otherwise required, counsel must request an extension of time to respond to the interrogatories from the court. For more information on seeking extensions of time generally from the court

Serving Responses

The same issues and requirements that apply to serving interrogatories apply to serving responses to interrogatories

- Sign the responses.
- Prepare and sign proof of service.
- Make copies of the signed responses, the client's verification (if any), and proof of service.
- Retain the original signed responses, verification (if any), and proof of service for counsel's file.
- **Not** file responses with the court or serve responses through the court's **Case Management/Electronic Case Filing** (CM/ECF) system.

Supplementing or Amending Answers

FRCP 26(e) requires a party who has responded to interrogatories to supplement or correct its response in a timely manner if either:

- The party learns that the response is incomplete or incorrect in some material respect, and the additional or corrective information has not otherwise been made known to the other parties during discovery or in writing.
- The court orders the party to supplement or correct its response.

(FRCP 26(e)(1)(A)-(B).)

This rule presumes that the responding party previously served proper, formal, complete, and sworn answers (*Villareal*, 266 F.R.D. at 211).

The responding party must execute a separate verification for any supplemental or amended answers (*Knights Armament Co. v. Optical Sys. Tech., Inc.*, 254 F.R.D. 463 (M.D. Fla. 2008); see also The "Under Oath" Requirement).

Motion to Compel: Drafting and Filing (OH)

This Practice Note discusses motions to compel discovery in Ohio litigation. It addresses motions to compel as to interrogatories, requests for production of documents, requests for admissions, deposition questions and third party discovery under the Ohio Civil Rules. It also addresses some differences among local rules that require parties to attempt to resolve discovery disputes without court intervention.

Contents

A motion to compel is a motion that seeks an order requiring another party or a non-party to provide discovery requested by the moving party. Motions to compel allow parties to ensure that they receive sufficient information and evidence from others concerning the case's relevant claims and defenses.

This Note focuses on how to draft and file motions to compel discovery authorized under the Ohio Civil Rules, as well as practical considerations for evaluating different types of motions to compel. This Note also discusses how to draft and file an opposition to a motion to compel, as well as a reply (where permitted by local rule).

This Note does not address in detail motions for protective orders or motions to quash subpoenas, which are motions that a respondent seeking to avoid discovery may file. This Note also does not discuss motions under Ohio Civ. R. 35 for a physical or mental examination of a person (commonly known as an IME).

General Considerations for a Motion to Compel

Courts generally prefer to stay out of the discovery process. (See 1994 Staff Note, Ohio Civ. R. 37 (stating that generally discovery is self-regulating and court intervention should be a last resort); *Nunez Vega v. Tivurcio*, 10th Dist. Franklin No. 14AP–327, 2014-Ohio-4588, ¶ 43.) The Ohio Civil Rules and many local rules require parties to informally attempt to resolve discovery disputes prior to filing a motion to compel. Counsel should carefully consider whether to file a motion to compel discovery, as the judge may expect the parties to resolve the dispute themselves.

Applicable Laws and Rules

Before drafting a motion to compel in an Ohio state court, counsel should review the applicable rules, including:

- The relevant Ohio Rules of Civil Procedure, including:
  - Ohio Civ. R. 37, which governs motions to compel answers to deposition questions and interrogatories as well as production of documents and ESI from parties;

- Ohio Civ. R. 45, which governs motions to compel production of documents and ESI from non-parties under a subpoena and authorizes sanctions for a non-party's failure to comply with a subpoena;
  - Ohio Civ. R. 26, which governs the scope of discovery; and
  - Ohio Civ. R. 30, 31, 33, 34 and 36, which govern the various types of discovery that parties may seek to compel.
- A court's local rules, particularly those involving:
  - general discovery practices;
  - the pre-motion requirements for parties to attempt to resolve discovery disputes;
  - the form of attorney statements reciting efforts to resolve the discovery dispute; and
  - supporting evidence for a motion to compel.
- The presiding judge's general guidelines and civil litigation preferences regarding motion and discovery practices.
- Discovery or case management orders in a particular case.

In addition, before filing any motion parties should always consult the Civil Rules and local rules regarding:

- How to properly format the motion papers, including:
  - paper size;
  - width of the margins;
  - line spacing; and
  - font size.
- Page or word limits.
- Methods of service and filing.

Ohio court websites usually provide links to their rules. Many judges publish their general guidelines or litigation preferences on their webpages, found through the court's website.

Potential Benefits and Risks of Filing a Motion to Compel

Before filing a motion to compel, counsel should consider the potential benefits and risks of the motion.

The potential benefits of a motion to compel include:

- Obtaining key evidence to support the party's claims and defenses or defeat the opposing party's position.
- Weakening the opposing party's credibility with the court.
- Recovering the expenses of preparing and filing the motion to compel if successful.
- Preserving arguments at trial and on appeal based on the party's failure to provide discovery.

However, filing a motion to compel has potential risks, which include:

- Losing credibility by bringing a weak motion.
- Annoying the court because the parties have failed to resolve the dispute.
- Losing an award of expenses to the opposing party.
- Triggering a retaliatory motion from the opposing party, such as a motion to compel or a motion for protective order.

Timing of the Motion to Compel

The Ohio Civil Rules do not specify when a party must file a motion to compel. When considering timing, however, counsel should note the discovery cutoff date. Some local rules provide that the discovery cutoff is the last date for counsel to approach the court with any motions regarding discovery. (See, for example, Loc. R. 3.05(E) of the Court of Common Pleas of Allen County, General Division; Loc. R. 47.02 of the Local Rules of Practice of the Franklin County Common Pleas Court, General Division.)

Even if the judge or a local rule does not explicitly require a party to file a motion to compel before the discovery cutoff, counsel should file her motion to compel:

- Shortly after the parties reaches an impasse, so there is not a significant delay between the discovery responses and the motion to compel.
- Sufficiently before trial to allow the requesting party to obtain and review the discovery if the court grants an order compelling discovery.

Requesting an Oral Hearing on the Motion to Compel

Ohio Civ. R. 7(B)(2) authorizes courts to decide motions on the briefs, without an oral hearing, and many courts prefer to decide motions in that manner. Counsel should keep this in mind when determining whether to request an oral hearing on the motion to compel. However, if a requesting party must file a motion to compel due to dilatory and noncompliant behavior, as opposed to a substantive dispute on a discovery issue, the movant may want to request an oral hearing to force the opponent to appear in front of the judge.

Courts vary on whether they permit oral argument for motions. Some courts:

- Allow oral argument upon written request (Loc. R. 14(C)(1)(a) of the Court of Common Pleas of Hamilton County, General Division).
- Only allow oral argument if the requesting party demonstrates the need for one (Loc. R. 5.1 of the Court of Common Pleas of Madison County, General Division).
- Do not allow oral argument unless ordered by the court (Loc. R. 5(A) of the Court of Common Pleas of Medina County, General Division).

Because courts vary significantly on whether and to what extent they permit oral argument, counsel should always check the court's local rules and the judge's guidelines or litigation preferences.

Evaluating Potential Motions to Compel

A party can move to compel most types of discovery authorized under the Ohio Civil Rules, including:

- Interrogatory answers (see Motions to Compel Interrogatory Answers).
- Document productions (see Motions to Compel Production of Documents by a Party).
- Request for admission (RFA) responses (see Motions to Determine Sufficiency of RFA Responses).
- Deposition testimony (see Motions to Compel Deposition Testimony).
- Third party discovery (see Motions to Compel Third Party Discovery).

The following sections provide information and considerations concerning each of these motions.

Motions to Compel Interrogatory Answers

The scope of discovery for interrogatories is broad. An interrogatory may relate to any matter, not privileged, that is relevant to the subject matter involved in the pending action, whether it relates to the claim or defense of the discovering party or of any other party. (Ohio Civ. R. 33(B) and Ohio Civ. R. 26(B)(1).)

Prior to filing a motion to compel answers to interrogatories, counsel must ensure that the number of interrogatories, including subparts, does not exceed the statutory limit. Ohio Civ. R. 33(A) limits the number of interrogatories to 40, with

any subpart of an interrogatory counting as a separate interrogatory. However, a few courts limit the number of interrogatories to fewer than 40. (See, for example, Summit County Loc. R. 17.01.)

Counsel should analyze various factors when determining whether to move to compel an interrogatory answer, including:

- The amount of information in the response. Incomplete or evasive answers are considered a failure to answer. (Ohio Civ. R. 37(A)(4).) An answer may be incomplete or evasive if it:
  - does not answer the question asked; or
  - does not include information that should be within the responding party's control.
- The use of boilerplate and vague objections. Each interrogatory objection must be specifically stated. (Ohio Civ. R. 33(A)(3).)
- The improper use of Ohio Civ. R. 33(C). A responding party can answer an interrogatory by identifying business records from which the answer can be derived, but only if the burden of deriving the answer is substantially the same for either party. (Ohio Civ. R. 33(C); *Jaric, Inc. v. Chakrof*, 63 Ohio App.3d 506, 512-13, 579 N.E.2d 493 (10th Dist.1989).)
- The timing of contention interrogatories, if the responding party has objected that the case is in its early stages. Ohio Civ. R 33(B) allows a court to order that contention interrogatories be answered later in the case.

Motions to Compel Production of Documents by a Party

As with interrogatories, the scope of discovery for document production requests is broad. A party may request production of documents and electronically stored information (ESI) regarding any matter, not privileged, that is relevant to the subject matter involved in the pending action, whether it relates to the claim or defense of the requesting party or of any other party. (Ohio Civ. R. 34(A) and Ohio Civ. R. 26(B)(1).) The responding party must produce information that is in its possession, custody or control. (Ohio Civ. R. 34(A).)

Ohio Civ. R. 34 applies only to parties. To obtain documents or ESI from a non-party, counsel must issue a subpoena under Ohio Civ. R. 45. (Ohio Civ. R. 34(C).)

A party responding to a request for production of documents must serve a written response. With respect to each item or category requested, the response must either:

- State that the party is producing documents as requested.
- State an objection to the request and specify the reasons. If the objection is to part of an item or category, the response must specify the objectionable part.

(Ohio Civ. R. 34(B)(1).)

The responding party must produce documents either as they are kept in the usual course of business, or organized and labeled to correspond with the categories in the request. (Ohio Civ. R. 34(B)(2).) If a request does not specify the form for producing ESI, the responding party must produce any ESI in the form in which it is ordinarily maintained or in a reasonably usable form. (Ohio Civ. R. 34(B)(3).)

The requesting party may move for an order under Ohio Civ. R. 37 with respect to any objection or other failure to respond to the request or any part of the request. (Ohio Civ. R. 34(B)(1).)

A motion to compel a party to produce documents and ESI may be appropriate when:

- ESI is not produced in the form requested. Under Ohio Civ. R. 34(B)(1), a party can object to the requested form of producing ESI, if it states the reasons for the objection and the form of ESI that it intends to use. The requesting party can then move for an order under Ohio Civ. R. 37.

- The responding party files a motion for protective order under Ohio Civ. R. 26(C).
- The responding party fails to produce documents within its possession, custody or control.
- The responding party unduly delays production of responsive documents.
- The responding party's document production identifies information or documents that the responding party refuses to produce.
- The responding party makes an improper claim of privilege as to documents. Under Ohio Civ. R. 26(B)(6)(a), a party objecting on grounds of privilege in response to discovery must:
  - expressly make the claim; and
  - provide a description of the nature of the documents, communications or things not produced that is sufficient to enable the requesting party to contest the claim.
- The responding party fails to provide a privilege log when claiming privilege as to certain documents. Some courts have held that Ohio Civ. R. 26(B)(6)(a) requires parties to produce a privilege log. (*Hartzell v. Breneman*, 7th Dist. Mahoning No. 10 MA 67, 2011-Ohio-2472, ¶ 19.)

Counsel should consider a motion to compel if the documents will help prove the requesting party's claims or defenses, or undermine the opposing party's claims or defenses.

Motions to Determine Sufficiency of RFA Responses

A party may serve upon any other party a written request for the admission of the truth of any matter, not privileged, that is relevant to the subject matter involved in the pending action, whether it relates to the claim or defense of the requesting party or of any other party. (Ohio Civ. R. 36(A) and Ohio Civ. R. 26(B)(1).) A request for admission (RFA) may relate to statements or opinions of fact or the application of law to fact, including the genuineness of any documents identified in the request. (Ohio Civ. R. 36(A).)

In responding to each RFA, a party must either:

- Respond with an admission, denial, or explanation of why the party cannot admit or deny the request. Counsel should note that:
  - if a party claims lack of information or knowledge as the reason for failing to admit or deny, the response must state that the party has made a reasonable inquiry and that information known or readily obtainable is insufficient to enable the party to admit or deny; and
  - when good faith requires that a party qualify an answer or deny only a part of the request, the party must specify so much of it as is true and qualify or deny the remainder.
- Object to the request.

(Ohio Civ. R. 36(A)(1)-(2).)

Ohio Civ. R. 37 does not authorize parties to file a motion to compel RFA answers. Rather, Ohio Civ. R. 36(A)(3) allows a party to file a motion challenging the responding party's objections or answers to RFAs. The court may:

- With respect to an objection:
  - determine that it is justified; or
  - order the party to serve an answer to the request.
- With respect to an answer that the court determines does not comply with Rule 36's requirements:
  - order the request admitted; or
  - require the party to serve an amended answer.
- Defer the final disposition of the request until a pretrial conference or designated time prior to trial.

(Ohio Civ. R. 36(A)(3).)

Unlike Ohio Civ. R. 37, Ohio Civ. R. 36 does not contain a requirement that the moving party make a reasonable effort to resolve the dispute before filing a motion to challenge RFA responses. Many courts' local rules, however, require parties to make extrajudicial attempts to resolve the issues before filing any discovery motion. (See, for example, Loc. R. 11.0(F) of the Court of Common Pleas of Cuyahoga County, General Division (requiring attempt to resolve issues as to any discovery procedure under Ohio Civ. R. 26 through Ohio Civ. R. 37).)

A motion under Ohio Civ. R. 36(A)(3) challenging RFA responses may be appropriate when:

- The responding party asserts a lack of knowledge even though the request concerns facts or information within its possession.
- The responding party disputes a fact that it has no basis to dispute.
- The responding party fails to admit the authenticity of a document that it produced.

If the court grants a requesting party's motion under Ohio Civ. R. 36(A)(3), the court will award the movant its reasonable expenses, including attorneys' fees, unless the opposition was substantially justified or other circumstances make an award of expenses unjust. (Ohio Civ. R. 36(A)(3), applying former Ohio Civ. R. 37(A)(4) (now Ohio Civ. R. 37(A)(5)).)

A motion under Ohio Civ. R. 36(A)(3) may not be necessary if a party does not respond to the requests within 28 days after service (or within such shorter or longer time as the court may allow). This is because the failure to serve a response results in the automatic admission of the matters requested. (Ohio Civ. R. 36(A)(1).) Once admitted, the matter is conclusively established unless the court grants a motion to withdraw or amend the admission. (Ohio Civ. R. 36(B); *Martin v. Martin*, 179 Ohio App.3d 805, 2008-Ohio-6336, 903 N.E.2d 1243, ¶ 14 (2nd Dist.).)

Note also that under Ohio Civ. R. 37(C), if a responding party fails to admit the truth of a matter requested (including the authenticity of a document), the requesting party after proving the matter may file a motion for the reasonable expenses, including attorneys' fees, of making the proof. A court must award the expenses unless the request was objectionable, good reason existed for the party's failure to admit, or the requested admission was not substantially important. (Ohio Civ. R. 37(C).)

Motions to Compel Deposition Testimony

Ohio Civ. R. 30(A) allows a party to take the deposition of a party or non-party witness by oral testimony, while Ohio Civ. R. 31(A) allows a party to take a deposition upon written questions. Depositions by written questions are rare in Ohio.

To obtain a deposition of a party, the requesting party serves a notice of deposition on all parties or their attorneys. (Ohio Civ. R. 30(A), (B)(1).) To obtain the deposition of a non-party, the requesting party must serve a subpoena. (Ohio Civ. R. 30(A) and Ohio Civ. R. 45.) For more information on noticing depositions in Ohio lawsuits, see Practice Note, Depositions: Noticing a Deposition (OH). For more information on deposition subpoenas in Ohio, see Practice Note, Subpoenas in State Court: Drafting a Subpoena (OH) and Practice Note, Subpoenas in State Court: Issuing and Serving a Subpoena (OH).

A motion to compel deposition testimony may be appropriate when:

- The opposing party fails to designate a witness in response to an Ohio Civ. R. 30(B)(5) deposition notice or presents a witness who is unprepared to testify on a designated deposition topic on behalf of the organization. (For more information on the requirements for preparing a Rule 30(B)(5) witness, see Practice Note, How to Prepare for and Successfully Defend a Deposition of an Entity Representative (OH).)
- An opposing party or its officer, director or managing agent fails to appear for a deposition after being served with proper notice. Ohio Civ. R. 37(D) also permits the noticing party to move for sanctions against the party who failed to appear without first obtaining an order compelling attendance at the deposition. (See Failure by a Party to Respond to

Discovery.)

- A non-party witness fails to appear for a deposition after being served with a proper subpoena. Under Ohio Civ. R. 45(E), the party may move for an order of contempt and an order compelling the witness to attend the deposition. (See, for example, 5 Ohio Jur. Pl. & Pr. Forms § 43:49 (2014 ed.).)
- A witness improperly refuses to answer a deposition question. (Ohio Civ. R. 37(A)(3).) In many cases, this may result from an improper instruction by opposing counsel. (For more on proper deposition objections and responding to improper objections, see Practice Note, Depositions: Preparing to Take a Deposition (OH).)

A motion to compel may be appropriate to obtain deposition testimony concerning information that may support the deposing party's claims and defenses or undermine the opponent's positions. The deposing party should consider moving to compel as to deposition questions where the witness or opposing counsel mistakenly believes that the information is protected by the attorney-client privilege or work product doctrine. (For information on attorney-client privilege and work product claims, see Practice Note, Litigating Attorney-Client Privilege and Work Product Claims (OH).

Motions to Compel Third Party Discovery

Ohio Civ. R. 45 allows a party to subpoena documents and ESI from a non-party (often called a document subpoena or subpoena *duces tecum*). A non-party served with a document subpoena may:

- Produce the requested information. Documents must be produced:
  - as they are kept in the usual course of business; or
  - organized and labeled to correspond with the categories in the subpoena.

(Ohio Civ. R. 45(D)(1).)

- Serve written objections to the requests. (Ohio Civ. R. 45(C)(2)(b).)
- File a motion to quash or modify the subpoena if it:
  - fails to allow a reasonable time to comply;
  - requires disclosure of privileged or otherwise protected matter and no exception or waiver applies;
  - seeks facts or opinions from a party's non-testifying, consulting experts; or
  - subjects a person to undue burden.

(Ohio Civ. R. 45(C)(3).)

If a non-party serves written objections in response to a document subpoena, the requesting party may file a motion to compel under Ohio Civ. R. 45(C)(2)(b). Any order compelling production must protect the non-party from significant expense resulting from production. (Ohio Civ. R. 45(C)(2)(b).)

A requesting party may move to compel production of ESI if the subpoenaed non-party resists production on the grounds of undue burden or expense. In opposing the motion, the non-party must show that the ESI is not reasonably accessible because of undue burden or expense. The court may nonetheless order production if the requesting party shows good cause. An order compelling production of ESI may specify the format, extent, timing, allocation of expenses and other conditions. (Ohio Civ. R. 45(D)(3).)

Motions for Discovery Sanctions

Failure to Comply with an Order Compelling Discovery

If a judge grants a party's motion to compel discovery, she will issue an order requiring the responding party to provide the requested discovery, usually identifying a deadline for providing the discovery. If the responding party does not comply with the discovery order, then the requesting party may seek sanctions under Ohio Civ. R. 37(B).

Rule 37(B)(1) allows a court to make "just" orders in response to a party's failure to comply with a discovery order, including but not limited to an order that:

- Establishes, in favor of the requesting party for purposes of the action, the matters related to the order to compel or any other designated facts.
- Prohibits the disobedient party from introducing designated matters into evidence or from supporting or opposing designated claims or defenses.
- Strikes out pleadings or parts of pleadings.
- Stays further proceedings until the order is obeyed.
- Dismisses the action or any part of it.
- Renders a default judgment against the disobedient party.

(Ohio Civ. R. 37(B)(1)(a)-(f).)

In addition, a court can make findings of contempt against:

- A deponent who fails to be sworn or to answer a question after being directed to do so by the court.
- A party (or its agent) who fails to obey any discovery order except an order to submit to a physical or mental examination under Ohio Civ. R. 35(A).

(Ohio Civ. R. 37(B)(1)(g).)

In addition to or instead of these sanctions, the court shall require the party failing to obey the discovery order or its advising attorney (or both) to pay the reasonable expenses, including attorneys' fees, caused by the failure, unless the court expressly finds that the failure was substantially justified or that other circumstances make an award of expenses unjust. (Ohio Civ. R. 37(B)(3).)

In evaluating the appropriateness of a discovery sanction, courts should consider both the posture of the case and a party's efforts preceding the noncompliance. The court should also balance the severity of the violation against the degree of possible sanctions. (*Bayes v. Toledo Edison Co.*, 6th Dist. Lucas No. L–03–1177, L–03–1194, 2004-Ohio-5752, ¶ 89.)

Failure by a Party to Respond to Discovery

If a party fails to respond to discovery entirely, the requesting party can file a motion for sanctions, bypassing a motion to compel. (Ohio Civ. R. 37(D).) Rule 37(D) applies when a party fails to:

- Appear for deposition.
- Serve answers or objections to interrogatories under Ohio Civ. R. 33.
- Serve a written response to a request for production under Ohio Civ. R. 34.

Thus, Ohio Civ. R. 37(D) provides a one-step method for immediate imposition of sanctions, upon motion, when a party fails to respond to discovery. (*Dafco, Inc. v. Reynolds*, 9 Ohio App.3d 4, 5, 457 N.E.2d 916 (10th Dist.1983).) Ohio Civ. R. 37(D) only applies:

- To parties.
- When there has been a complete or nearly total failure of discovery. (*Davis v. Byers Circle Investments, Inc.*, 10th Dist. Franklin No. 89AP-878, 1990 WL 34753, *3 (Mar. 29, 1990) (quoting *Fox v. Studebaker-Worthington, Inc.*, 516 F. 2d 989, 995 (8th Cir., 1975), construing the parallel Fed. R. Civ. P. 37(d)).)

A party must make effort to resolve the discovery dispute before filing a Rule 37(D) motion for sanctions (see Ohio Civ. R. 37(D)(1)(b)). For additional information about this "conference requirement," see Pre-Motion Attempts to Resolve the Dispute.)

A court can award the same sanctions against a party who fails to respond to discovery that it can award under Ohio Civ. R. 37(B)(1)(a)-(f) against a party who fails to comply with an order compelling discovery, but contempt sanctions are not available. (See Ohio Civ. R. 37(D)(3).) For additional information, see Failure to Comply with an Order Compelling Discovery.)

Absent exceptional circumstances, a court may not impose sanctions on a party for failing to provide electronically stored information (ESI) lost as a result of the routine, good-faith operation of an electronic information system (Ohio. Civ. R. 37(E)). The court may consider the following factors in determining whether to impose sanctions in these circumstances:

- Whether and when any obligation to preserve the information was triggered.
- Whether the information was lost as a result of the routine alteration or deletion of information that attends the ordinary use of the system in issue.
- Whether the party intervened in a timely fashion to prevent the loss of information.
- Any steps taken to comply with any court order or party agreement requiring preservation of specific information.
- Any other relevant facts.

(Ohio Civ. R. 37(E).)

Failure by a Non-party to Respond to a Subpoena

Ohio Civ. R. 45(E) provides for sanctions against a non-party who fails to obey a subpoena without an adequate excuse. Sanctions under Rule 45(E) include:

- Finding the non-party in contempt of court.
- Requiring the non-party (or the non-party's attorney) who frivolously resists discovery to pay the reasonable expenses, including reasonable attorneys' fees, of the party seeking discovery.

R.C. 2705.02(C) similarly provides that a witness who fails to obey a subpoena can be held in contempt.

Pre-Motion Attempts to Resolve the Dispute

Both the Ohio Civil Rules and many courts' local rules require parties or persons to make efforts to resolve a discovery dispute prior to approaching the court with a motion to compel. This section of the Note discusses the pre-motion requirements of Ohio Civ. R. 37(A)(1) and some local rules.

Good Faith Effort to Confer under Ohio Civ. R. 37(A)(1)

Ohio Civ. R. 37(A)(1) requires a movant in good faith to confer or attempt to confer with the party or person resisting discovery to resolve the discovery matter before filing a motion under Rule 37. This requirement applies to a motion to compel under Ohio Civ. R. 37(A)(3).

Ohio Civ. R. 37(A)(1) does not apply to:

- Motions to compel production of documents or ESI from a third party by a subpoena, governed by Ohio Civ. R. 45(C)(2)(b).
- Motions for sanctions for failure to obey a subpoena under Ohio Civ. R. 45(E).
- Motions to determine the sufficiency of request for admission (RFA) responses, governed by Ohio Civ. R. 36(A)(3).

However, even as to these motions, a court's local rules may require a party to engage in extrajudicial efforts to resolve the discovery dispute before filing a motion. (See Local Rule Requirements.)

A prior version of this Rule required the moving party to make a reasonable effort to resolve the discovery dispute (Editor's and Revisor's 2016 Notes to Ohio Civ. R. 37). The new Rule and comments do not state whether or how the good faith requirement will differ from the reasonableness requirement. Ohio case law addressing the prior rule did not explicitly define "reasonable effort" but required something more than a single, insubstantial attempt to resolve a dispute. For example, one court found that a single telephone call, without a description in the motion to compel of the substance of the call or when it was placed, did not satisfy the conference requirement. (*Dewey L. Tackett Builders v. Casey*, 4th Dist. Pike No. 99CA637, 2001-Ohio-2674, 2001 WL 803016, *4.) In contrast, another court held that a series of letters between the attorneys demonstrating an impasse constituted reasonable efforts. (*Wrinch v. Miller*, 183 Ohio App.3d 445, 2009-Ohio-3862, 917 N.E.2d 348, ¶ 33 (9th Dist.).)

Local Rule Requirements

Many courts' local rules impose requirements on attorneys to attempt to resolve a discovery dispute out of court before filing a motion, which may be more stringent than the Rule 37(A)(1) "reasonable effort" requirement. Examples include rules requiring parties to:

- "Exhaust all extrajudicial means" for the resolution of their differences (Loc. R. 14(D) of the Court of Common Pleas of Hamilton County, General Division) or "exhaust among themselves all extrajudicial means for the resolution of differences" (Loc. R. 6.04(D) of the Court of Common Pleas of Butler County, General Division).
- Make a "diligent effort" to solve the problem informally (Gr. Co. C.P.R. 2.09(IV)(A)) or to resolve the impasse without involvement from the court (Mont. Co. C.P.R. 2.09(B)(4)). One court found that a moving party who only made one email follow-up to opposing counsel regarding a discovery dispute did not make a diligent effort under the rule. (*Dixon v. Kettering Medical Center Network, Mont. C.P. No.* 2013CV00063, 2013 WL 8695352, *1, (July 15, 2013) (construing Montgomery County rule).)
- Engage in "personal consultation and sincere attempts to resolve differences." The party seeking discovery must initiate the personal consultation. (Loc. R. 11.0(F) of the Court of Common Pleas of Cuyahoga County, General Division.)
- Make "every effort" to resolve the discovery dispute by agreement prior to filing discovery motions with the court. (Loc. R. 47.01 of the Local Rules of Practice of the Franklin County Common Pleas Court, General Division; see *Lewis v. Caulfield*, Franklin C.P. No. 12CV0201629, 2012 WL 10130269, *1 (Oct. 17, 2012).)
- Initiate a conference (in person or by telephone) with the judge and the attorney, unrepresented party, or person from whom discovery is sought, so that the parties and the court can discuss the discovery dispute and seek informal resolution. (Loc. R. 3.05(B)(2) of the Court of Common Pleas of Allen County, General Division.)

When attempting to resolve a discovery dispute informally with the opposing party, counsel should make more than one attempt if the first one is unsuccessful. Counsel should document any telephone conversations and generally use written

correspondence to set out the parties' positions. On a discovery motion, the correspondence will help demonstrate the attempts to resolve the issue without court intervention.

Necessary Papers for the Motion to Compel

On a motion to compel discovery, the moving party must demonstrate the facts surrounding the parties' discovery dispute as well as the legal authority supporting its right to the requested information. This section of the Note discusses the necessary documents included in a motion to compel.

Many courts have specific rules regarding the formatting of motions. A motion to compel:

- Must be formatted correctly (See Formatting the Necessary Papers).
- Typically contains:
  - the motion (see Motion);
  - a memorandum of law (see Memorandum of Law);
  - supporting evidence including the discovery at issue (see Supporting Evidence); and
  - a proposed order, if required by the court (see Proposed Order).
  - a Rule 37(A)(1) certification (see Certification of Good Faith Effort to Confer).

Although not required under the Ohio Civil Rules, some local rules require a notice of hearing, even where the hearing is a "non-oral hearing." (See Motion.)

For additional information about the required motion papers, see Practice Note, Motion Practice in Ohio State Court.

Formatting the Necessary Papers

The motion document and a proposed order (if one is required) should contain the caption of the case and a signature block (the proposed order's signature block should be a line on which the judge or magistrate can sign). In Ohio practice, the memorandum of law is often attached to or incorporated into the motion. In that case, the attorney usually does not include a new caption on the memorandum, but the memorandum usually has its own signature line. (See Motion and Memorandum of Law.)

The Ohio Civil Rules do not specify how to format and file the statement of the attorney reciting attempts to resolve the discovery dispute, or the evidence supporting the motion to compel. Some local rules dictate how to format and file one or both of these. (See Supporting Evidence.) If the attorney statement is a separately filed document, it needs its own caption and signature block.

Omit Personal Identifiers

When filing motions, counsel (and parties) must omit personal identifiers from the motion and accompanying documents, and submit them separately to the court. (Ohio Sup. R. 45(D).)

"Personal Identifiers" include:

- Social security numbers (except for the last four digits).

- Financial account numbers, including debit card, charge card and credit card numbers.
- Employer and employee identification numbers.
- A juvenile's name in an abuse, neglect or dependency case, except for the juvenile's initials or a generic abbreviation such as "CV" for "child victim."

(Ohio Sup. R. 44(H).)

Some courts provide a form for counsel to use to identify "personal identifiers." (See, for example, Preble Co. C.P. Personal Identifier form.) Counsel should check the court's local rules regarding redaction.

For more on redacting personal identifiers, see Practice Note, Court Records, Privacy and Redaction (OH).

Caption

The caption is located near the top of the first page of a litigation document. A document's caption must include:

- The court name.
- The title of the action.
- The case number.
- The title of the document.

(Ohio Civ. R. 10(A).)

Though not required by the Ohio Civil Rules, local rules may require that the caption include the name of the judge assigned to the case. (See, for example, Loc. R. 8.0(A) of the Court of Common Pleas of Cuyahoga County, General Division.) The judge's name is typically located on the right side of the caption below the case docket number.

The document name is typically located below the judge's name on the right side of the caption. On a motion to compel, the moving party should make the motion's name specific to both:

- The party from whom the moving party requested discovery.
- The type of discovery at issue, particularly in a case with multiple parties and more than one type of discovery served.

For example, a party could name the document "Motion of [Plaintiff/Defendant] [PARTY NAME] to Compel Answers to Interrogatories from [Plaintiff/Defendant] [PARTY NAME]."

The caption goes on the first page of all pleadings, motions and other legal papers. Counsel should review local rules for placement requirements. It is common practice to leave a blank space along the top margin for file stamping by the clerk. For example, the Court of Common Pleas of Allen County requires that the top right hand corner of the first page have a 3" by 3" space left blank for the clerk to file stamp the date and time of filing. (Loc. R. 2.04 of the Court of Common Pleas of Allen County, General Division.)

Signature Block

Under Ohio Civ. R. 11, a motion to compel, opposition and reply, if allowed, must be signed by at least one attorney of record in the attorney's name. By signing a motion, opposition or reply, an attorney certifies that to the best of the attorney's knowledge, information and belief, there is good ground to support the document and it is not being interposed for delay.

evidence, without oral arguments from counsel). (See, for example, Loc. R. 5(B) of the Court of Common Pleas of Licking County, General Division.)

If required under a court's local rules, a notice of hearing should generally contain the date and time of hearing and be served on all parties or their counsel, but the procedures vary by local court. For this reason, counsel should always consult local rules regarding hearing and any notice-of-hearing requirements.

Memorandum of Law

Most courts require a party to support a motion with a memorandum of law. (See, for example, Loc. R. 5(A)(1) of the Court of Common Pleas of Adams County, General Division.)

Unless the motion to compel involves a particularly complicated legal issue, such as the application of a privilege, counsel can keep the memorandum of law relatively brief, without many citations to legal authorities. In fact, some local rules emphasize this point. (See, for example, Loc. R. 14(D)(2) of the Court of Common Pleas of Hamilton County, General Division (memorandum supporting a motion to compel should be concise, addressing only relevant issues and generally not exceeding ten pages).)

A memorandum of law typically contains:

- Facts (see Facts).
- A legal argument (see Legal Argument).
- A conclusion (see Conclusion).

Counsel should attach the memorandum of law to the motion, or incorporate the memorandum of law into the motion. (See, for example, Loc. R. 6.02(A) of the Court of Common Pleas of Butler County, General Division.) Counsel should consult the relevant local rules to determine if the court has a preference.

Counsel commonly incorporate the memorandum of law into the motion document after the signature line appearing on the motion, usually starting on a new page. The memorandum does not need its own caption, but counsel will generally place the title "Memorandum of Law" in bold at the beginning of the memorandum. The memorandum has its own signature line in accordance with Ohio Civ. R. 11.

Facts

This section of the memorandum provides the court with relevant facts. For a motion to compel, the facts will generally relate to:

- The proper service of the discovery requests.
- The inadequate discovery responses, or the failure to respond, that triggered the discovery dispute.
- The requesting party's attempts to resolve the matter without court intervention. Whether or not they also appear in the memorandum, such facts must be set out in a statement by the moving party's attorney under Ohio Civ. R. 37(A)(1).

Legal Argument

The legal argument section of the memorandum cites to legal authority to explain to the court why the respondent should be compelled to answer the requested discovery or produce the relevant information. The moving party should demonstrate to the court why the discovery responses are inadequate under the rules. In most cases, the moving party will base its motion on:

- Ohio Civ. R. 37(A)(3), covering motions to compel:
  - parties and non-parties to answer deposition questions;
  - parties to answer interrogatories; and
  - parties to produce documents and ESI.
- Ohio Civ. R. 45(C)(2)(b), covering motions to compel non-parties to produce documents and ESI.
- Ohio Civ. R. 36(A)(3), covering motions regarding the sufficiency of RFA responses.

Absent a complicated legal issue, counsel may need only a few citations to legal authorities, since courts generally prefer concise discovery motions.

Conclusion

The conclusion is a short paragraph at the end of the memorandum that:

- Reiterates the moving party's request to compel the respondent to provide answers to discovery or produce information.
- Refers back to the reasons set out in the memorandum.

Supporting Evidence

The moving party should submit the discovery requests and responses at issue to the court to support the motion to compel. Ohio Civ. R. 5(D) generally prohibits the filing of discovery requests and responses, but contains an exception for discovery documents filed in support of a motion.

The Civil Rules do not prescribe how to file discovery documents as supporting evidence for a motion. Some local rules outline procedures for doing so. For example, some courts require that the discovery documents be:

- Attached to the motion to compel (Loc. R. 6(G) of the Court of Common Pleas of Geauga County, General Division).
- Accompanied by a certification from counsel that they are being filed for use as evidence in consideration of a motion (Mont. Co. C.P.R. 2.09(E)(2)).

If the local rules do not address the filing requirements, counsel may use one of the common methods to file the discovery requests and responses:

- Attach them to the motion to compel and supporting memorandum.
- Attach them to the attorney's affidavit, which also outlines the extrajudicial efforts to resolve the dispute.
- File them separately with the court, attaching a notice of filing to the discovery. (See, for example, 5 Ohio Jur. Pl. & Pr. Forms § 43:76 (2014 ed.).)

Counsel must serve copies of any discovery documents that she is filing with the motion, evidenced by a certificate of service. If counsel attaches the discovery to the motion itself or to an affidavit, these documents typically have their own certificate of service and that will suffice for the attached discovery. But if counsel is separately filing the discovery, for example through a notice of filing, the document must contain a certificate of service. (See Proof of Service.)

Proposed Order

The Ohio Civil Rules do not require the parties to submit a proposed order with a motion to compel. Some local rules, however, require proposed orders to be submitted with any motion. (See, for example, Loc. R. 4.02(D) of the Court of

Common Pleas of Defiance County, General Division.) The proposed order should contain language granting the motion to compel, and should either state a date when the responding party must provide the discovery or have a blank space for the court to enter a date.

Since under Ohio Civ. R. 37(A)(5) some courts may conduct an oral evidentiary hearing before awarding expenses and fees to the prevailing party, counsel may want to consider leaving a blank space for the court to enter the date and time for such a hearing if one is desired. (See for example, 5 Ohio Jur. Pl. & Pr. Forms § 43:85 (2014 ed.). See also Reasonable Expenses Assessed Against Losing Party.)

Counsel should always check local rules to determine if they dictate any specific requirements when submitting a proposed order.

Certification of Good Faith Effort to Confer

Ohio Civ. R. 37(A)(1) requires parties to include with any Rule 37 motion to compel a certification that the moving party has in good faith conferred or attempted to confer with the non-producing person or party to resolve the matter prior to seeking court intervention. Note that local rules may impose more stringent requirements for parties to attempt to resolve the dispute prior to seeking court intervention. (See Local Rule Requirements.)

Some courts require the attorneys to submit:

- An affidavit. For example:
  - Loc. R. 14(D)(2)(a) of the Court of Common Pleas of Hamilton County, General Division, requires counsel to submit an affidavit stating what extrajudicial means have been attempted to resolve differences; and
  - Gr. Co. C.P.R. 2.09(IV) requires the affidavit to include the specific times and methods of attempted informal resolution.
- A certificate of counsel attached to the motion to compel that states the extrajudicial means employed to resolve the dispute. (Loc. R. 6.04(D) of the Court of Common Pleas of Butler County, General Division.)
- A certificate of impasse, attached to or made part of the discovery motion, that includes the specific times and methods of attempted informal resolution. (Mont. Co. C.P.R. 2.09(C)(1).)
- A written statement to the court advising that after personal consultation and sincere attempts to resolve differences, the parties are unable to reach an accord. (Loc. R. 11.0(F) of the Court of Common Pleas of Cuyahoga County, General Division (statement must recite the matters that remain in dispute and the date, time and place of the parties' conference).)

Some attorneys will describe the conference or attempts to confer in the certification and attach to it any correspondence regarding the discovery dispute.

Serving and Filing

For determining when a party "makes" a motion, the Ohio Civil Rules generally focus on the time of service. Under Ohio Civ. R. 5(D), counsel must file documents that are required to be served (after the complaint) within three days of service. Courts will not consider filed documents that are not accompanied by a certificate of service, indicating the date and manner of service on all parties. (Ohio Civ. R. 5(B)(4).) These rules clarify that counsel must serve the documents either before or contemporaneously with filing.

The Ohio Civil Rules do not specify any time deadlines for serving or filing a motion to compel. Note that some local rules, however, require all discovery motions to be filed before the discovery cutoff. (See, for example Loc. R. 3.05(E) of the Court of Common Pleas of Allen County, General Division.)

file.
- Check the court's hours of operation, and leave plenty of time for the filing agent to file the documents. Many Ohio courts close by 4:00 or 4:30 p.m. (best to file in the morning).
- Ensure the filing agent has a cell phone and that an attorney familiar with the case is available for a call should any issues arise.

Some courts allow paper filing via facsimile. (See, for example, Gr. Co. C.P.R. 2.04.) Counsel should consult the court's local rules to determine proper filing techniques to file the motion by fax.

Counsel must serve copies of the motion to compel, memorandum of law (which may be attached to or incorporated in the motion), statement reciting efforts to resolve the discovery dispute, proposed order (if any), and supporting evidence on all counsel of record and unrepresented parties by either:

- Handing the documents to the person.
- Leaving them:
  - at the person's office with a clerk or other person in charge or, if no one is in charge, in a conspicuous place in the person's office; or
  - if the person has no office or the office is closed, at the person's dwelling or usual place of abode with someone of suitable age and discretion who resides there.
- Mailing them to the person's last known address by US mail (service is complete upon mailing).
- Delivering them to a commercial carrier service for delivery to the person's last known address within three calendar days (service is complete upon delivery to the carrier).
- Leaving them with the clerk of court if the person has no known address.
- Sending them by electronic means to a fax number or e-mail address provided in accordance with Ohio Civ. R. 11 by the attorney or party to be served (service is complete upon transmission, but service is not effective if the serving party learns that the documents did not reach the person served).

(Ohio Civ. R. 5(B)(2)(a)-(f).)

Counsel should consult the court's local rules to determine whether they must deliver courtesy copies of the motion to compel to the court after filing. (See, for example Loc. R. 4.1 of the Common Pleas of Clermont County, General Division.)

For more information on serving and filing in a paper format jurisdiction, see Filing Checklist: General Paper Filings (OH).

For more information on serving motion papers, see Practice Note, Serving Court Documents Subsequent to the Complaint.

Proof of Service

The motion to compel (with attached or incorporated memorandum of law) must be accompanied by a proof of service, commonly referred to as a "certificate of service." Further, the attorney statement reciting efforts to resolve the discovery dispute and the supporting evidence must each contain a certificate of service, unless they are incorporated into or attached to a document with its own certificate of service (such as the motion to compel or an attorney affidavit).

The certificate of service is generally placed at the end of the document and includes:

- The date of service.
- The manner of service (such as first class mail).
- The division of Ohio Civ. R. 5(B)(2) by which the service was made, for example:
  - electronically through the court's transmission facilities under Rule 5(B)(2)(f); or
  - by mail to the last known address under Rule 5(B)(2)(c).

Ohio courts require either:

- Electronic filing (see, for example, Mont. Co. C.P.R. 1.15).
- Paper filing (see, for example, Loc. R. 2.2(A) of the Court of Common Pleas of Columbiana County, General Division, which does not allow for e-filing or fax filing).

Some courts are transitioning into electronic filing for all cases, establishing deadlines for different types of cases to convert to electronic filing. Counsel should check the local rules to determine whether the jurisdiction is in a transitional phase, to ascertain the filing requirements for the particular case type. (See, for example, Loc. R. 5.07 of the Court of Common Pleas of Butler Country, General Division.)

Filing and Serving Electronically

Ohio Civ. R. 5(E) allows courts to make local rules to control e-filing of documents. Before e-filing a motion to compel, counsel should:

- Ensure they have registered with the court's electronic filing system, which usually requires a login and password.
- Learn how to navigate the electronic filing system.
- Review the court's local rules for electronic filing for guidance on:
  - formatting;
  - timing; and
  - size and page limits.
- Allow ample time for filing.
- Check the court's electronic docket to verify that all parties can receive the motion via electronic service. Ohio Civ. R. 5(B)(3) allows a party to use the court's transmission facilities to serve the document, if the local rule of the jurisdiction authorizes electronic notification service (for example, Loc. R. 7.04(H)(4)(c)(i) and 7.04(H)(2)(vii) of the Court of Common Pleas of Summit County, General Division, allowing parties to serve by electronic notification sent through the court's e-filing system).
- Ensure that any party not registered to receive electronic service with the court is served according to another method under Ohio Civ. R. 5(B)(2) (see Filing and Serving in Paper Format).
- Check the local rules for sample language to include in the certificate of service for electronic filings (see, for example, Mont. Co. C.P.R. 1.15(H)(4)(c)(ii)).
- Check the local rules to determine whether the court requires hand delivery of courtesy copies of the motion after filing.

Filing and Serving in Paper Format

To file a motion to compel in the traditional paper format, counsel should instruct the filing agent to go to the court with the original documents and filing fee in hand. To ensure that the filing runs smoothly, counsel should:

- Make certain the court does not require electronic filing instead of or in addition to filing in paper format.
- Make sure the document format complies with local rules (including its rules on paper size, font size, font type, captions and signatures).
- Have lead counsel of record sign all of the documents.
- Give the filing agent the original for filing.
- Provide sufficient copies of the signed documents so the clerk can file stamp one or more to return a copy for counsel's

- The signature of the attorney of record.
- The names and addresses of the attorneys or parties served.

(Ohio Civ. R. 5(B)(4).)

Note that the proof of service can also be its own, separately filed document, although common practice is to include it in the document served. (Ohio Civ. R. 5(B)(4).)

Also note that although Rule 5(B)(4) requires that the proof of service identify the division of Rule 5(B)(2) by which the party served the document, common practice in Ohio is simply to state the method of service. (See *Bader v. Ferri*, 3rd Dist. Allen No. 1-13-01, 2013-Ohio-3074.)

In electronic filing jurisdictions, counsel should check local rules to determine the specific language appropriate for an electronic certificate of service. (See, for example, Mont. Co. C.P.R. 1.15(H)(4)(c).)

Oppositions and Replies

Once a party seeking discovery has filed a motion to compel, the respondent has an opportunity to oppose the motion, and some courts allow the moving party to file a reply. This section of the Note describes both oppositions and replies.

Serving and Filing an Opposition

The opposition to a motion to compel generally needs to include:

- A memorandum of law in opposition to the motion.
- Any supporting evidence not submitted by the moving party.

The opposition need not include a statement outlining extrajudicial attempts to resolve the dispute, but counsel may want to do so to clarify or dispute the attorney statement filed by the moving party.

Counsel sometimes file, together with an opposition to a motion to compel, a motion for protective order under Ohio Civ. R. 26(C), asking the court to issue an order limiting or precluding the requested discovery. Counsel should review Ohio Civ. R. 26(C) and related authority for additional information. Note that as with a Rule 37 motion, Rule 26(C) does require a motion for protective order to include a statement reciting the reasonable efforts made to resolve the matter with the discovering party.

Service

Local rules generally set out the amount of time in which counsel must serve an opposition to a motion, which is typically within a specified number of days from the service of the motion. (See, for example, Loc. R. 14(B) of the Court of Common Pleas of Hamilton County, General Division (opposition must be served ten days from the date the memorandum in support of the motion was served).) However, under some local rules, the time to submit an opposition is tied to the filing, not service, of the motion. (See, for example, Loc. R. 9(II) of the Court of Common Pleas of Lorain County, General Division (deadline for an opposition is 14 days after the day on which the motion was filed).)

If the local rules do not provide a response time for oppositions, Ohio Civ. R. 6(C) provides that responses must be served within 14 days after service of the motion, unless a court order specifies otherwise. (Ohio Civ. R. 6(C).)

Counsel should check the local rules to ensure that the opposition papers conform to page and formatting requirements, which are often the same as the requirements for moving papers.

Filing

Typically, when opposing a motion counsel must file the opposition document(s) with the court within three days of serving the document(s) on the moving party. (See Ohio Civ. R. 5(D).) Note, however, that according to the 2015 Staff Note to Ohio Civ. R. 6, this rule does not apply if a local rule specifies a different time for filing a response to a motion. (See 2015 Staff Note, Ohio Civ. R. 6.) Therefore, before computing the response filing time using Rule 5(D), counsel must first ensure that the local rules do not specify a different time for filing.

Note that common practice is for counsel to serve and file documents contemporaneously. Often, this occurs automatically in e-filing jurisdictions.

Time Computation

In computing the deadline for an opposition, counsel should not count the actual day the motion was served (or the day it was filed, if a local rule calculates the response time from the date of filing). (Ohio Civ. R. 6(A).) Counsel should include the last day of the time period in the computation, unless it falls on a Saturday, Sunday or legal holiday, in which case the period runs until the end of the next day that is not a Saturday, Sunday or legal holiday. (Ohio Civ. R. 6(A).) Further, when the time period to respond is less than seven days, counsel may skip Saturdays, Sundays and legal holidays in the time computation. (Ohio Civ. R. 6(A).)

Under Ohio Civ. R. 6(D), when a party has the right or is required to do some act within a prescribed period after being served with a document and it is served by mail or commercial carrier service, three days are added to the prescribed period.

Thus, a respondent typically may add three days to the time to respond to a motion to compel if by rule the response period is triggered by service and the movant serves the motion by:

- Mail (under Ohio Civ. R. 5(B)(2)(c)).
- Commercial carrier service (under Ohio Civ. R. 5(B)(2)(d)).

Note that this three-day grace period under Ohio Civ. R. 6(D) does not apply when service is by any means other than mail or commercial carrier service, including electronic service under Ohio Civ. 5(B)(2)(f). (2012 Staff Note, Ohio Civ. R. 6.)

Serving and Filing a Reply

Ohio courts generally take one of the following approaches to reply briefs:

- Reply briefs are allowed (see, for example, Loc. R. 11.01 of the Court of Common Pleas of Ross County, General Division).
- Reply briefs are only allowed by leave of court upon a showing of good cause (see, for example, Loc. R. 11.0(D) of the Court of Common Pleas of Cuyahoga County, General Division).
- Reply briefs are not allowed (see, for example, Loc. R. 7.14(A) of the Court of Common Pleas of Summit County,

General Division).

Reply briefs typically are:

- Shorter than moving or opposition briefs.
- Limited to addressing the legal arguments set out in the opposition papers.

Counsel should check the local rules and judge's rules to:

- Ensure that reply papers are permitted.
- Determine the amount of time allowed for serving reply papers, which is generally less than allowed for opposition briefs.
- Ensure that their reply brief conforms to page and formatting requirements.

If a local rule or court order does not provide a time for serving replies, Ohio Civ. R. 6(C) provides that replies must be served within seven days after service of the response to the motion.

If the responding party serves the response by mail or commercial carrier service, Ohio Civ. R. 6(D) generally allows the moving party to add three days to the time to serve the reply when the reply period is triggered by service of the response.

Absent a local rule to the contrary, Ohio Civ. R. 5(D) gives counsel an additional three days after serving the reply memorandum to file it with the court. (See 2015 Staff Note, Ohio Civ. R. 6.)

Reasonable Expenses Assessed Against Losing Party

A court must award reasonable expenses, including attorneys' fees, to the prevailing party on a motion to compel, unless the court finds that any of the following are true:

- The movant filed the motion before attempting in good faith to obtain the discovery without court action.
- The losing party's position with respect to the motion was substantially justified.
- Other circumstances make an award of expenses unjust.

(Ohio Civ. R. 37(A)(5)(a).)

Thus, unless one of the above exceptions applies, if the motion to compel is:

- Granted, the court awards the reasonable expenses of obtaining the order to the moving party.
- Denied, the court awards the reasonable expenses of opposing the motion to the non-moving party.
- Granted in part and denied in part, the court may apportion the reasonable expenses incurred in relation to the motion among the parties and persons in a just manner.

(Ohio Civ. R. 37(A)(5).)

The court may require the payment of reasonable expenses to be made by the losing party or its attorney or both. (Ohio Civ. R. 37(A)(5).)

Ohio Civ. R. 37(A)(5) is not applicable to motions to compel production of documents or ESI from subpoenaed non-parties. Ohio Civ. R. 45(E), which governs such motions, provides that a person or her attorney who frivolously resists discovery under a subpoena may be required to pay the reasonable expenses, including reasonable attorneys' fees, of the party seeking the discovery. In turn, if the requesting party fails to take reasonable steps to avoid imposing undue burden or expense on a

person subject to a subpoena, the court may impose sanctions on the requesting party or its attorney, which may include lost earnings and reasonable attorneys' fees. (Ohio Civ. R. 45(E) and Ohio Civ. R. 45(C)(1).)

Under Ohio Civ. R. 37(A)(5), the court awards the expenses after "giving an opportunity to be heard." It is not clear whether this phrase requires the court to conduct an oral hearing, or merely allows the parties to be heard on the motion documents and supporting evidence (a non-oral hearing). Generally, courts may determine motions without oral hearings and upon the parties' written submissions. (Ohio Civ. R. 7(B)(2).) A party who wants an oral hearing on the reasonable expenses available under Ohio Civ. R. 37(A)(5) should request one, and the court likely has discretion to grant or deny the request.

If the trial judge decides to conduct an oral hearing, she can hear testimony and review exhibits submitted to support the attorneys' fees and expenses related to preparing the motion or opposition. (See *Bobb Chevrolet, Inc. v. Dobbins*, 4th Dist. Ross No. No. 01CA2621, 2002-Ohio-4256, ¶ 30.) If the judge instead chooses to review the parties' written submissions without an oral hearing, counsel may be required to submit a statement of fees and costs incurred in connection with the motion. (See, for example, 5 Ohio Jur. Pl. & Pr. Forms § 43:25 (2014 ed.).)

Note, some courts hold that when refusing to award expenses under Ohio Civ. R. 37(A)(5), a trial court must make a finding on the record as to one of the statutory exceptions. (See *Shikner v. S & P Solutions*, 8th Dist. Cuyahoga No. 86291, 2006-Ohio-1339, ¶ 15; but see *Babb v. Ford Motor Co., Inc.*, 41 Ohio App. 3d 174, 181, 535 N.E.2d 676 (8th Dist.1987) (finding that the court is not required to express its findings in refusing to award expenses).)

Subpoenas in State Court: Responding to a Subpoena (FL)

This Practice Note provides guidance on how to respond to discovery and trial subpoenas in Florida. It addresses the steps to take before responding to a subpoena, how to comply with a subpoena, and methods for objecting to a subpoena, such as with a motion to quash or a motion for protective order.

Contents

J

Consequences for Disobeying a Subpoena

Parties use subpoenas in civil practice to obtain testimony or documents, or both, and other tangible information, usually from non-parties. When an individual or an entity is served with a subpoena, they must respond appropriately or risk liability for sanctions.

This Note examines what steps to take when responding or objecting to a subpoena to meet the requirements of the applicable rules and statutes, while preserving the recipient's rights and interests. Where applicable, it addresses the different requirements for a subpoena that seeks documents or other tangible information (also called a subpoena *duces tecum*) and for a subpoena seeking testimony at a deposition, hearing, or trial (testimonial subpoena).

Initial Considerations When Responding to a Subpoena

After a client is served with a subpoena, counsel should take certain steps to ensure a proper and timely response, including:

- Understanding the applicable statutes and rules (see Review the Applicable Law).
- Calendaring the deadlines for responding (see Calendar the Deadlines to Respond or Object).
- Preserving responsive documents (see Preserve Responsive Documents).
- Deciding how to respond to the subpoena (see Determine Potential Responses).

Review the Applicable Law

The Florida Rules of Civil Procedure address several issues related to responding to a subpoena, such as:

- The scope of **discovery**, including withholding privileged matter (Fla. R. Civ. P. 1.280(b)(1)).
- Objections to producing documents during discovery (Fla. R. Civ. P. 1.410(e)(1) and 1.351(c)).
- Objections to producing documents at trial (Fla. R. Civ. P. 1.410(c)).
- Motions to quash, modify, or condition a subpoena (for example, the court may require the issuing party to pay expenses to the subpoena recipient as a condition of requiring the recipient to produce documents in response to the subpoena) (Fla. R. Civ. P. 1.410(c), (e)(1)).
- Motions for a protective order (Fla. R. Civ. P. 1.280(c)).

Additional rules address issues relating to enforcement of a subpoena, including:

- The consequences of disobeying a subpoena, including punishment for contempt of court (Fla. R. Civ. P. 1.410(f)).
- Motions to compel compliance with the subpoena (Fla. R. Civ. P. 1.380(a)).

Calendar the Deadlines to Respond or Object

Counsel should calendar the appropriate deadlines to ensure a timely response or objection to the subpoena.

Determine the Deadline to Respond

The subpoena must state the time and place of compliance and identify whether the subpoena seeks testimony, production of evidence, or both (Fla. R. Civ. P. 1.410). Counsel should calendar the compliance date (sometimes called the return date) immediately on receiving the subpoena, and contact the issuing party to negotiate any necessary extensions before the compliance date. Counsel should obtain or confirm any extensions in writing.

Determine the Deadline to Object

Counsel also should calendar the deadline for serving and filing:

- Objections (see Time for Objecting to a Subpoena).
- A motion to quash, modify, or condition the subpoena (see When to Make the Motion to Quash, Modify, or Condition).
- A motion for protective order (see When to Make the Motion for Protective Order).

These deadlines depend on the type of subpoena served.

Preserve Responsive Documents

A subpoena recipient has a duty to identify and preserve responsive documents and information after receiving a subpoena *duces tecum* (see *Gayer v. Fine Line Const. & Elec., Inc.*, 970 So. 2d 424, 426 (Fla. 4th DCA 2007)). The recipient should immediately take steps to preserve responsive documents and information to avoid a potential claim of spoliation of evidence (*Royal & Sunalliance v. Lauderdale Marine Ctr.*, 877 So. 2d 843, 844-45 (Fla. 4th DCA 2004)).

For more information about the duty to preserve relevant documents and information in Florida, see Practice Note, Implementing a Litigation Hold (FL).

Determine Potential Responses

A subpoena recipient may respond in several ways. Depending on the circumstances of the case, the recipient may:

- Comply with the subpoena and provide the requested testimony or documents, or both (see Complying with a Subpoena).
- Serve and file written objections to a document subpoena (see Objecting to a Subpoena).
- Move to quash, condition, or modify the subpoena (see Moving to Quash, Modify, or Condition a Subpoena).
- Move for a protective order (see Moving for a Protective Order).

Complying with a Subpoena

If there are no grounds for objections, complying with a subpoena may be the most appropriate course of action.

Complying with a Document Subpoena

A subpoena recipient who chooses to comply with a document subpoena (also called a subpoena *duces tecum*) without objecting must produce all non-privileged materials in the recipient's possession, custody, or control that are responsive to the subpoena.

The recipient should ensure that the requested materials arrive at the location stated in the subpoena (typically, the office of the attorney issuing the subpoena) on or before the subpoena's compliance date (or, if counsel obtained an extension in writing, on or before the extension date).

To respond properly to a document subpoena, a recipient also should consider:

- The form and organization of the document production (see Form and Organization of Production and Form and Organization of ESI).
- Whether to withhold documents (see Withholding Documents).
- The costs of producing documents (see Document Production Costs).

Form and Organization of Production

The Florida Rules of Civil Procedure do not specify the form or organization of documents produced in response to a document subpoena, except for **electronically stored information** (ESI) (see Form and Organization of ESI).

However, when parties produce documents in response to requests for production under Fla. R. Civ. P. 1.350, they must:

- Produce the documents as they are kept in the usual course of business.
- Identify the documents to correspond with the categories in the request.

Based on this rule, Florida practitioners generally produce documents in response to subpoenas as they are kept in the usual course of business.

Unless the subpoena directs the recipient to make original documents available for inspection and copying where they are usually maintained, producing accurate copies of the documents is sufficient (Fla. R. Civ. P. 1.310(f)(1), 1.351(c), and 1.410(e)(1)). The recipient is not required to surrender the original materials (Fla. R. Civ. P. 1.351(b); Fla. R. Civ. P. Form 1.922).

Although not required, the subpoena recipient should consider labeling the documents with **Bates numbers** for easy identification and reference.

Form and Organization of ESI

If the subpoena seeks ESI, the issuing party may specify the form in which the subpoena recipient should produce ESI. For example, the issuing party may request that the subpoena recipient produce ESI in PDF, TIFF, or native format and include certain metadata.

If a subpoena requests ESI but does not specify a form of production, the subpoena recipient must produce the ESI either in:

- The form or forms in which it is ordinarily maintained.
- A reasonably usable form.

(Fla. R. Civ. P. 1.410(c).)

For more information on handling and producing ESI, see Practice Note Overview, E-Discovery in Florida: Overview (FL).

Withholding Documents

A subpoena recipient must consider whether to withhold certain documents or materials from the production. Common grounds for withholding documents include:

- The attorney-client privilege (§ 90.502, Fla. Stat.)
- Attorney work-product (Fla. R. Civ. P. 1.280(b)(4)).
- Confidential information and trade secrets (Fla. R. Civ. P. 1.280(c)(7) and § 90.506, Fla. Stat.).

Unlike parties to Florida litigation, a non-party is not required to serve a privilege log (see Fla. R. Civ. P. 1.280(b)(5); *Westco, Inc. v. Scott Lewis' Gardening & Trimming, Inc.*, 26 So. 3d 620, 623 (Fla. 4th DCA 2009)). A non-party should assert a claim of privilege by either serving written objections or moving for a protective order.

Confidentiality and trade secret objections are usually addressed by a confidentiality agreement or stipulated protective order to prevent disclosure of sensitive information while still producing the subpoenaed materials.

Document Production Costs

The recipient of a document subpoena (without deposition) may require the issuing party to pay the reasonable costs of producing documents in response to the subpoena before production (Fla. R. Civ. P. 1.351(c)).

However, the recipient of a document subpoena for deposition can only require the issuing party to pay the reasonable costs of production by filing a motion and obtaining a court order (Fla. R. Civ. P. 1.410(c)). In practice, counsel should request reimbursement informally and only file the motion if necessary.

Complying with a Testimonial Subpoena

To comply with a testimonial subpoena, the recipient must appear for the deposition, hearing, or trial on the date, time, and place stated in the subpoena.

For depositions, the parties and the witness typically agree in advance to the date, time, and place. However, a deposition subpoena can only compel the attendance of a non-party witness in the county:

- Where the person resides.
- Where the person works.
- Where the person transacts business.
- That a court order designates.

(Fla. R. Civ. P. 1.410(e)(2).)

If a subpoena specifies a place outside of these geographical limits, counsel for the recipient should contact the issuing party in writing and request that the party change the location. If the issuing party refuses, counsel should file a motion to quash the subpoena (see Moving to Quash, Modify, or Condition a Subpoena).

Complying with a Subpoena for a Corporate Representative Deposition

A party may depose a corporation or other business entity either by:

- Naming as the deponent a particular officer or director.
- Naming as the deponent a corporation, partnership, association, or governmental agency, and stating with reasonable particularity the topics of examination. This is commonly referred to as a corporate representative deposition. (Fla. R. Civ. P. 1.310(b)(6).)

When a subpoena requests a corporate representative deposition, the organization:

- Must designate one or more representatives to testify on its behalf.
- May, but is not required to, state the matters on which each designated person will testify, if the organization designates more than one representative.
- Must prepare its representative(s) to testify on the topics identified in the subpoena based on matters known or reasonably available to the organization from documents, past employees, or other sources of information.

(Fla. R. Civ. P. 1.310(b)(6).)

Although a party may issue a deposition subpoena to a corporate representative, a trial subpoena must identify a specific person as the subpoena recipient. A party may not issue a trial subpoena to a corporate representative. (*Dopson-Troutt v. Novartis Pharm. Corp.*, 295 F.R.D. 536, 539 (M.D. Fla. 2013); see *Franklyn S., Inc. v. Riesenbeck*, 166 So. 2d 831, 832 (Fla. 3d DCA 1964) (absent square holding on point by Florida courts, Florida courts rely on federal court's construction of parallel federal rule).)

Objecting to a Subpoena

In response to a document subpoena, the recipient may serve (but need not file with the court) written objections to the document requests (Fla. R. Civ. P. 1.351(c) and 1.410(e)).

Time for Objecting to a Subpoena

The time for objecting to a subpoena depends on the type of document subpoena served.

Objecting to a Document Subpoena for Deposition

To properly object to document requests in a document subpoena that also seeks a deposition (sometimes called a subpoena *duces tecum* for deposition), the recipient must serve written objections either:

- Within ten days after service of the subpoena.
- Before the time for compliance, if the time is less than ten days after service of the subpoena.

(Fla. R. Civ. P. 1.410(e)(1).)

When a subpoena recipient objects to a document subpoena for deposition, the issuing party is not entitled to the subpoenaed documents without first obtaining a court order (Fla. R. Civ. P. 1.410(e)(1)).

Although serving written objections stays the obligation to produce evidence in response to the subpoena, it does not stay the obligation to appear for deposition. If the recipient seeks to stay the deposition, the recipient must file a motion to quash or motion for protective order. (See Moving to Quash, Modify, or Condition a Subpoena and Moving for a Protective Order.)

Objecting to a Document Subpoena Without Deposition

A recipient served with a document subpoena that does not also seek a deposition (sometimes called a subpoena *duces tecum* without deposition) may serve an objection to the subpoena any time before the deadline to produce the subpoenaed materials (Fla. R. Civ. P. 1.351(c)).

An objection under Rule 1.351 is self-executing, meaning that an objection by a subpoena recipient immediately relieves the recipient from any obligation to produce the evidence. Moreover, the rule does not require the recipient to specify the basis of the objection. To discover the basis for the objection and obtain the requested documents, the issuing party must depose the records custodian. The issuing party **cannot** seek a ruling on the objection without first taking the deposition. (See *Patrowicz v. Wolff*, 110 So. 3d 973, 974 (Fla. 2d DCA 2013); *Morgan, Colling & Gilbert, P.A. v. Pope*, 756 So. 2d 201, 201-02 (Fla. 2d DCA 2000).)

Although Rule 1.351(c) does not expressly require written objections, the subpoena recipient should serve objections in writing before the time for production.

Grounds for Objecting to a Document Subpoena

A variety of different grounds exists for objecting to a document subpoena. Common objections include:

- Objections to the form of the subpoena, such as:
  - a lack of authority to issue the subpoena (Fla. R. Civ. P. 1.410(a));
  - improper location for the deposition (Fla. R. Civ. P. 1.410(e)(2));
  - improper service (Fla. R. Civ. P. 1.410(d)); and
  - failure to include the witness fee (§§ 92.142(1) and 92.151, Fla. Stat.).
- Objections to the substance of the subpoena, such as because the subpoena:
  - seeks information not within the scope of discovery (Fla. R. Civ. P. 1.280(b)(1));
  - is unreasonable and oppressive (Fla. R. Civ. P. 1.410(c));
  - seeks documents protected by **attorney-client privilege**, **work product**, or other recognized privilege (Fla. R. Civ. P. 1.280(b)(1), (4));
  - seeks documents containing confidential or proprietary information (Fla. R. Civ. P. 1.280(c));
  - seeks protected trade secrets (§ 90.506, Fla. Stat.; Fla. R. Civ. P. 1.280(c)); and
  - fails to describe the documents sought with reasonable particularity (*Palmer v. Servis*, 393 So. 2d 653, 654-55 (Fla. 5th DCA 1981)).
- Objections to the production of ESI based on undue burden or cost because the source is not reasonably accessible (Fla. R. Civ. P. 1.280(d)(1) and 1.410(c)).

These objections also may serve as grounds for a motion for protective order or a motion to quash, modify, or condition a subpoena (see Moving to Quash, Modify, or Condition a Subpoena and Moving for a Protective Order). However, many practitioners prefer to serve objections rather than a motion to put the burden on the issuing party to seek relief from the court to compel the production.

Failing to Timely Seek Court Relief

A subpoena recipient's failure to timely seek court relief from a document subpoena may waive objections to requests for documents that are otherwise within the scope of discovery. However, privilege objections and objections to matters outside the scope of discovery are not waived unless the protected information is actually disclosed. (See *Truly Nolan Exterminating, Inc. v. Thomasson*, 554 So. 2d 5, 5 (Fla. 3d DCA 1989); *Ins. Co. of N. Am. v. Noya*, 398 So. 2d 836, 838 (Fla. 5th DCA 1981).)

Moving to Quash, Modify, or Condition a Subpoena

If the subpoena recipient has appropriate grounds to challenge a subpoena seeking documents or testimony, it may move to quash, modify, or condition the subpoena (Fla. R. Civ. P. 1.410(c)).

Grounds for the Motion to Quash, Modify, or Condition

A recipient may challenge a subpoena with a motion to:

- Quash the subpoena.
- Modify the subpoena's scope.
- Condition compliance with the subpoena (for example, by requiring the issuing party to prepay the reasonable cost of producing any documents sought).

(Fla. R. Civ. P. 1.410(c).)

The grounds for obtaining an order to quash, modify, or condition a subpoena include that:

- The subpoena is oppressive and unreasonable (Fla. R. Civ. P. 1.410(c)).
- The subpoena is too indefinite for the recipient to respond (*Vann v. State*, 85 So. 2d 133, 136 (Fla. 1956)).
- No witness fees were tendered at the time of service (§§ 92.142(1) and 92.151, Fla. Stat.).
- There are technical deficiencies on the face of the subpoena, such as the failure to include all of the information required by Fla. R. Civ. P. 1.410.
- The subpoena sets the location for compliance for a location other than those authorized by Fla. R. Civ. P. 1.410(e)(2).
- The subpoena was improperly served (*Garfinkel v. Katzman*, 76 So. 3d 40, 41 (Fla. 4th DCA 2011)).
- The court lacks jurisdiction (*Sucarte v. Office of Comm'r*, 129 So. 3d 1112, 1114 (Fla. 3d DCA 2013)).
- The subpoena seeks ESI that is not reasonably accessible because of undue costs or burden (Fla. R. Civ. P. 1.410(c)).

A recipient **may not** move to quash a subpoena on the ground that the information or material sought is irrelevant to the underlying action (*Dade Cty. Med. Ass'n v. Hlis*, 372 So. 2d 117, 121 (Fla. 3d DCA 1979)).

Who May Make the Motion to Quash, Modify, or Condition

A motion to quash, modify, or condition a subpoena may be made by:

- The subpoena recipient (Fla. R. Civ. P. 1.410(c); *Dade Cty. Med. Ass'n v. Hlis*, 372 So. 2d 117, 121 & n. 5 (Fla. 3d DCA 1979)).
- A party on behalf of a subpoena recipient on grounds the subpoena is unreasonable and oppressive to the recipient (*Sunrise Shopping Ctr., Inc. v. Allied Stores Corp.*, 270 So. 2d 32, 34 (Fla. 4th DCA 1972)).

Where to Make the Motion to Quash, Modify, or Condition

A party or subpoena recipient must file a motion to quash, modify, or condition a subpoena in the court where the action is pending (Fla. R. Civ. P. 1.410(c)).

When to Make the Motion to Quash, Modify, or Condition

A party or subpoena recipient must file a motion to quash, modify, or condition a subpoena promptly, and no later than the time specified in the subpoena for compliance (Fla. R. Civ. P. 1.410(c)).

A subpoena recipient's failure to seek timely court relief from a document subpoena may waive objections to requests for documents that are otherwise within the scope of discovery (see Failing to Timely Seek Court Relief).

Available Relief on a Motion to Quash, Modify, or Condition

A court may grant a motion to quash in whole or in part and may issue an order:

- Quashing the subpoena in its entirety.
- Modifying the objectionable portions of the subpoena.
- For a document subpoena that also seeks a deposition, quashing the document production portion of the subpoena but allowing the deposition of the non-party (*Sunrise Shopping Ctr., Inc. v. Allied Stores Corp.*, 270 So. 2d 32, 34-35 (Fla. 4th DCA 1972)).
- Conditioning an appearance or production on the issuing party's compliance with certain requirements. For example, the court may require the issuing party to pre-pay the reasonable costs of production (Fla. R. Civ. P. 1.410(c) and 1.351(c)).

Although the court may condition a subpoena recipient's production of documents and ESI on the issuing party's pre-payment to the recipient of reasonable costs, those costs do not include attorney's fees (*Attorney's Title Ins. Fund, Inc. v. Landa-Posada*, 984 So. 2d 641, 643 (Fla. 3d DCA 2008); *Expeditions Unlimited, Inc. v. Rolly Marine Servs., Inc.*, 447 So. 2d 453 (Fla. 4th DCA 1984)).

Moving for a Protective Order

In response to a subpoena, the recipient may make a motion for a protective order under Fla. R. Civ. P. 1.280(c) instead of (or in combination with) a motion to quash or modify under Fla. R. Civ. P. 1.410(c).

Grounds for the Motion for Protective Order

A court may enter a protective order to prevent annoyance, embarrassment, oppression, or undue burden or expense (Fla. R. Civ. P. 1.280(c)). The movant must show good cause to obtain a protective order (*Towers v. City of Longwood*, 960 So. 2d 845, 848 (Fla. 5th DCA 2007)).

Grounds for relief include:

- Undue burden, such as a burdensome date or location for compliance (Fla. R. Civ. P. 1.280(c); *Cady v. Laws*, 341 So. 2d 1022 (Fla. 4th DCA 1977)).

- Undue expense to the recipient (Fla. R. Civ. P. 1.280(c)).
- Disclosure of privileged information or materials protected by work product or other recognized protections (Fla. R. Civ. P. 1.280(b)(6), (c)(4)).
- Disclosure of confidential or trade secret information (Fla. R. Civ. P. 1.280(c)(7); § 90.506, Fla. Stat.).
- Disclosure of other sensitive information, such as personal financial information (*Calvo v. Calvo*, 489 So. 2d 833, 834 (Fla. 3d DCA 1986)).
- Production of information outside the scope of discovery (Fla. R. Civ. P. 1.280(b)(1); *Peisach v. Antuna*, 539 So. 2d 544, 546 (Fla. 3d DCA 1989)).

For ESI, the court **must** issue a protective order to limit otherwise permissible discovery if:

- The discovery sought is unreasonably cumulative or duplicative.
- The discovery can be obtained from another source or in another manner that is:
  - more convenient;
  - less burdensome; or
  - less expensive.
- The burden or expense of the discovery outweighs its likely benefit considering:
  - the needs of the case;
  - the amount in controversy;
  - the parties' resources;
  - the importance of the issues at stake in the action; and
  - the importance of the discovery in resolving the issues.

(Fla. R. Civ. P. 1.280(d)(2).)

Who May Make the Motion for Protective Order

Both a non-party subpoena recipient and the parties to the litigation may seek a protective order (Fla. R. Civ. P. 1.280(c)).

Where to Make the Motion for Protective Order

A party or subpoena recipient must file the motion in the court where the action is pending (Fla. R. Civ. P. 1.280(c)).

When to Make the Motion for Protective Order

Fla. R. Civ. P. 1.280(c) does not specify the time to file a motion for a protective order. However, the filing of a motion for protective order does **not** automatically stay the time for complying with a subpoena in Florida (see *Momenah v. Ammache*, 616 So. 2d 121 (Fla. 2d DCA 1993); *Stables v. Rivers*, 559 So. 2d 440 (Fla. 1st DCA 1990)). Therefore, counsel should file the motion sufficiently before the compliance date to allow time to obtain a ruling on the motion.

If the deadline for compliance does not leave time to obtain a ruling, the subpoena recipient or counsel should contact the issuing party as soon as possible to negotiate an extension of the time or to attempt to resolve the issue, as the failure to seek timely court relief from a document subpoena may waive objections to requests for documents that are otherwise within the scope of discovery (see Failing to Timely Seek Court Relief).

Counsel must make a good faith attempt to resolve the dispute before bringing the motion. The motion must include a certificate of conference stating that a good faith attempt was made to resolve the dispute before seeking court intervention (Fla. R. Civ. P. 1.280(c); Fla. R. Civ. P. 1.380(a)(4)). Counsel should check the court's local rules, which may impose additional conference requirements (for example, FL ST 9 J CIR SECTION 13).

For more information on certificates of conference, see Standard Clause, Certificate of Conference (FL).

Available Relief on a Motion for Protective Order

The types of relief available on a motion for protective order is broader than the types of relief available for a motion to quash, modify, or condition a subpoena. Trial courts also have broad discretion in deciding whether to issue protective orders (*Katzman v. Rediron Fabrication, Inc.*, 76 So. 3d 1060, 1065 (Fla. 4th DCA 2011)). The court may, for good cause, issue an order to protect a party or person by:

- Disallowing the discovery.
- Allowing the discovery only on specified terms and conditions, such as designating the time and place for the discovery.
- Allowing discovery only by a different method than the one the issuing party selected.
- Precluding inquiry into certain matters or limiting the scope of discovery to certain matters.
- Designating the persons that may be present while the discovery is conducted.
- Requiring that a deposition be sealed and opened only on court order.
- Requiring that a trade secret or other confidential research, development, or commercial information not be disclosed or be disclosed only in a designated way.
- Requiring that the parties simultaneously file specified documents or information enclosed in sealed envelopes, to be opened only as the court directs.

(Fla. R. Civ. P. 1.280(c).)

If the discovery sought includes ESI, the court has discretion to:

- Grant the motion if the moving party or person shows that the ESI sought or the format requested is not reasonably accessible because of undue burden or cost.
- Deny the motion and order the ESI discovery, despite the showing of undue burden or cost, if the party seeking discovery shows good cause.
- Specify conditions of the ESI discovery, including ordering that the party seeking discovery pay some or all of the expenses that the person producing the discovery incurred.

(Fla. R. Civ. P. 1.280(d)(1).)

In addition to substantive relief, Rule 1.280(c) authorizes an award of reasonable expenses depending on the outcome of the motion for protective order. Specifically:

- If the court grants the motion, the party or person against whom the protective order is entered **must** pay the movant's reasonable expenses incurred in obtaining the order, which may include attorneys' fees, unless the court finds:
  - the movant failed to certify in the movant's motion that the movant made a good faith effort to obtain the relief sought without involving the court;
  - the opposition to the motion was substantially justified; or
  - other circumstances exist that make awarding expenses unjust.
- If the court denies the motion, the moving party **must** pay the other party or person's reasonable expenses incurred in

opposing the motion, which may include attorneys' fees, unless the court finds:
  - the motion was substantially justified; or
  - other circumstances exist that make awarding expenses unjust.
- If the court grants the motion in part and denies it in part, Rule 1.380(a)(4) permits the court to apportion the reasonable expenses among the parties and persons.

(Fla. R. Civ. P. 1.380(a)(4).)

Consequences for Disobeying a Subpoena

A recipient who fails to comply with an otherwise valid subpoena without adequate excuse can be held in contempt and subjected to fines or imprisonment (Fla. R. Civ. P. 1.410(f)). The party issuing the subpoena should first file a motion to compel and obtain an order requiring the recipient to comply with the subpoena. If the recipient disobeys the order, the issuing party may move for contempt sanctions. However, if the recipient filed an objection to a document subpoena without deposition, the issuing party must first depose the records custodian before seeking relief from the court (see Objecting to a Document Subpoena Without Deposition).

Subpoenas in State Court: Enforcing a Subpoena (FL)

A Practice Note that addresses how to enforce a subpoena in a Florida civil action when the witness fails to comply. This Note examines the different motions that the issuing party may file to obtain compliance with a subpoena, including motions to compel and motions for contempt, and remedies available to the party enforcing a subpoena.

Contents

A party may use a subpoena to obtain testimony (testimonial subpoena) or documents (subpoena *duces tecum*) from non-party witnesses. However, witnesses may not always comply with a subpoena. This Note examines the steps a party that issues a subpoena (issuing party) may take to enforce it when the witness:

- Ignores the subpoena.

and contact the clerk of the circuit court to determine the procedure for opening a miscellaneous action, filing the motion, and obtaining a hearing on it.

In practice, counsel do not always follow this procedure and often file the motion to compel in the pending case even if the deposition is scheduled in a different county. If the witness opposes the motion to compel without raising a venue objection, the witness waives the objection (*Calderbank v. Cazares*, 435 So. 2d 377, 378 n.1 (Fla. 5th DCA 1983)).

If the deposition takes place outside of Florida, the laws of the forum where the deposition takes place typically govern the procedure for filing a motion to compel compliance with the subpoena (*Greenlight Fin. Servs., Inc. v. Union Am. Mortg., Inc.*, 971 So. 2d 983, 985 (Fla. 3d DCA 2008)).

When to Make the Motion

There is no specific time during which a party must move to compel compliance with a deposition subpoena. The best practice is to file the motion as soon as possible after the witness's non-compliance to ensure sufficient time to obtain a ruling and conduct the deposition before the discovery period closes.

If the motion is based on a failure to answer questions at a deposition, counsel may choose either to complete the deposition or adjourn it before filing a motion to compel (Fla. R. Civ. P. 1.310(d) and 1.380(a)(2)).

Counsel must give reasonable notice of a motion to compel discovery (Fla. R. Civ. P. 1.380(a)). The Florida Rules of Civil Procedure do not define "reasonable notice," but most Florida circuit courts have administrative orders or local rules specifying a minimum number of days (for example, FL ST 11 J CIR 1-06-09(1)(a); FL ST 20 J CIR 2.20(IV)(B)(1)). Providing at least five days' notice typically is sufficient.

Burden on the Motion

The party seeking to compel a witness's deposition testimony has the burden of showing the discovery sought is relevant or reasonably calculated to lead to the discovery of admissible evidence (*Calderbank v. Cazares*, 435 So. 2d 377, 379 (Fla. 5th DCA 1983)).

Counsel also should be prepared to address issues raised in any related motions from the witness, such as motions to quash or for protective order, even if those motions are not set for hearing at the same time.

Available Relief

A trial court has broad discretion in discovery matters and may issue any order it finds necessary, including entry of a protective order or an order imposing conditions on compliance with the subpoena (Fla. R. Civ. P. 1.380(a)(2)). For example, the court may compel a witness to appear for a deposition but limit the time or location of the deposition. (*Krypton Broad. v. MGM-Pathe Comm's Co.*, 629 So. 2d 852, 856 (Fla. 1st DCA 1993), disapproved on other grounds, *Allstate Ins. Co. v. Langston*, 655 So. 2d 91, 94-95 (Fla. 1995);*Am. Funding, Ltd. v. Hill*, 402 So. 2d 1369, 1371 (Fla. 1st DCA 1981).)

A court also can award reasonable expenses under Florida Rule of Civil Procedure 1.380(a)(4), depending on the disposition of the motion. If the court:

- Grants the motion, then the witness **must** pay the moving party's expenses, which may include attorneys' fees, unless:

    - the movant failed to make a good faith attempt to resolve the dispute;
    - the witness's opposition was substantially justified; or
    - other circumstances making an expense award unjust.
- Denies the motion, then the moving party **must** pay the witness's expenses, which may include attorneys' fees, unless:
    - the motion was substantially justified; or
    - other circumstances make awarding expenses unjust.
- Grants the motion in part and denies it in part, then the court may apportion the expenses.

(Fla. R. Civ. P. 1.380(a)(4).)

The court can only award expenses and attorneys' fees related to obtaining the court order or opposing the motion. The court cannot award expenses or attorneys' fees incurred in attempting to take a deposition. (*Liebreich v. Church of Scientology Flag Serv. Org., Inc.*, 855 So. 2d 658, 660 (Fla. 2d DCA 2003).)

Ex Parte Motions to Compel Discovery

A motion to compel discovery generally requires notice to the other parties and all affected persons (Fla. R. Civ. P. 1.380(a)). However, under limited circumstances, some courts rule on a motion to compel on an **ex parte** basis without a hearing. For example, the 17th Judicial Circuit allows *ex parte* motions to compel when the witness both:

- Completely fails to respond or object to the subpoena.
- Has not requested an extension of time.

(FL ST 17 J CIR LOCAL RULE NO. 10A (¶ 13).)

Counsel should consult the court's local rules and administrative orders for the availability of *ex parte* proceedings.

Moving for Contempt Sanctions After Non-Compliance with a Deposition Subpoena

Counsel should seek contempt sanctions if a witness disobeys an order granting a motion to compel compliance with the deposition subpoena (Fla. R. Civ. P. 1.380(a), (b)). Counsel sometimes seek contempt sanctions without first filing a motion to compel if the witness fails to comply with a subpoena without filing any objections or a motion challenging the subpoena (see Fla. R. Civ. P. 1.410(f)).

Types of Contempt

Contempt may be civil or criminal, depending on the character and purpose of the sanction imposed (*Parisi v. Broward Cty.*, 769 So. 2d 359, 364 (Fla. 2000); *Parsons v. Wennet*, 625 So. 2d 945, 947 (Fla. 4th DCA 1993)).

Civil contempt is remedial in nature (*Parisi*, 769 So. 2d at 364). Its purpose is to preserve and enforce the rights of the parties and to compel compliance with a court's order (*Lewis v. Nical of Palm Beach, Inc.*, 959 So. 2d 745, 752 (Fla. 4th DCA 2007); *Parsons*, 625 So. 2d at 947).

Criminal contempt punishes a person or party for violating the authority of the court (*Parsons*, 625 So. 2d at 947; *Lewis*, 959 So. 2d at 752). Criminal contempt requires proof beyond a reasonable doubt that the individual **intended** to disobey the court (*Tide v. State*, 804 So. 2d 412 (Fla. 4th DCA 2001)). Criminal contempt is either direct (in the judge's presence) or indirect (outside the judge's presence) (*Bank of N.Y. v. Moorings At Edgewater Condo. Ass'n, Inc.*, 79 So. 3d 164, 167 (Fla. 2d DCA

2012)). Courts generally only impose criminal contempt sanctions for disobeying a deposition subpoena in extraordinary circumstances, such as after repeated violations of court orders to appear for the deposition.

Grounds for the Motion

A party seeking compliance with a subpoena for deposition may request contempt sanctions if:

- The witness fails to comply with an otherwise valid subpoena without asserting valid objections or other adequate excuse (Fla. R. Civ. P. 1.410(f)).
- The witness fails to be sworn for deposition or answer a deposition question after the court instructs the witness to do so (Fla. R. Civ. P. 1.380(b)(1)).
- The witness fails to obey a court order (*Parsons*, 625 So. 2d at 947).

How to Make the Motion

For civil contempt proceedings, due process requires notice and an opportunity to be heard (*Parsons*, 625 So. 2d at 947). To comport with due process, the motion should set out the essential facts constituting the contempt, including details of service of the subpoena and the witness's failure to comply with the subpoena or court order. Counsel should attach:

- An affidavit supporting the facts set out in the motion.
- A copy of the order or subpoena with which the witness failed to comply.
- A proposed order stating:
  - that the witness willfully failed to comply with the order or subpoena;
  - the facts supporting the order;
  - that the court finds the witness in contempt;
  - the sanctions imposed (see Available Remedies); and
  - that the witness has the opportunity to purge the contempt and avoid sanctions by complying with the conditions set out in the order (for example, by sitting for the deposition).

Counsel should file and serve the motion and a notice of hearing on all parties to the case and arrange for the non-compliant witness to be personally served to satisfy due process requirements. Counsel should check the court's local rules and administrative orders for additional procedural requirements.

If counsel seeks criminal contempt sanctions, which Florida Rule of Criminal Procedure 3.840 governs, counsel must include:

- A request for an order to show cause why the noncompliant witness should not be held in criminal contempt.
- A proposed order to show cause that:
  - informs the witness that the witness is subject to criminal contempt sanctions;
  - states the essential facts of the contempt charge; and
  - states the time and place of the show cause hearing and leaves sufficient time for the witness to prepare the witness's defense.

(Fla. R. Crim. P. 3.840; *Wendel v. Wendel*, 958 So. 2d 1039, 1040 (Fla. 1st DCA 2007).)

If the witness does not respond or provides inadequate proof of compliance at the hearing on the motion for civil contempt or the show cause hearing, the court may issue an order holding the witness in contempt and imposing sanctions.

Where to Make the Motion
Counsel should file the motion for contempt in the same circuit court that issued the order compelling compliance (Fla. R. Civ. P. 1.380(b)(1) and 1.410(f)).

If counsel seeks contempt sanctions before filing a motion to compel, counsel should file the motion for contempt in the circuit court from which counsel issued the subpoena (Fla. R. Civ. P. 1.410(f)).

When to Make the Motion
Although the Florida Rules of Civil Procedure and the Florida Rules of Criminal Procedure do not specify a time for bringing a motion for contempt, counsel should file the motion as soon as practicable to ensure sufficient time to serve notice of the motion, obtain a ruling, and take the deposition before the discovery cutoff.

Available Remedies
Courts have broad discretion in imposing contempt sanctions (*Alan v. State*, 39 So. 3d 343, 345 & n.1 (Fla. 1st DCA 2010)). The same conduct may be the subject of both civil and criminal proceedings, but the available sanctions vary based on the type of contempt (*Parisi*, 769 So. 2d at 363-64). However, courts typically are more willing to grant civil contempt because the purge provision required in civil contempt orders gives the witness the ability to avoid the sanctions.

Civil contempt sanctions include:

- **Fines**. When a court imposes a fine as a sanction for civil contempt, the fine:
  - is limited to the actual damage that the injured party sustains from the discovery violation, if the fine is intended to compensate the movant for its losses (*H.K. Dev., LLC v. Greer*, 32 So. 3d 178, 185 (Fla. 1st DCA 2010); *Levine v. Keaster*, 862 So. 2d 876, 880 (Fla. 4th DCA 2003));
  - is not limited to actual damages and the court must consider the financial resources of the witness, if the fine is intended as a coercive fine to encourage the witness to comply with the court order (*Parisi*, 769 So. 2d at 366); and
  - must include a purge provision, which allows the witness to avoid the fine by complying with the court order (*Lewis*, 959 So. 2d at 752). Imposing a fixed fine that the court suspends pending the witness's compliance with a clear directive is an appropriate purge provision (*Huber v. Disaster Sols., LLC*, 180 So. 3d 1145, 1150-51 (Fla. 4th DCA 2015)).
- **Imprisonment**. When a trial court imposes imprisonment as a sanction for civil contempt:
  - the purpose of the imprisonment must be to coerce compliance, not punishment (*Parsons*, 625 So. 2d at 947);
  - the order imposing imprisonment must include a purge provision (*Jones v. Ryan*, 967 So. 2d 342, 344 (Fla. 3d DCA 2007));
  - the trial court must make a finding that the witness has the ability to comply with the purge conditions (*Bargiel v. Colt Studio, Inc.*, 901 So. 2d 315, 317 (Fla. 4th DCA 2005)); and
  - the witness is not entitled to a jury trial (*Lussy v. Fenniman*, 763 So. 2d 1110, 1111 (Fla. 4th DCA 1999)).
- **Attorney's fees.** When a court awards attorney's fees, the court must make findings regarding:
  - the time reasonably expended on the contempt proceedings (*Levine*, 862 So. 2d at 880);
  - the reasonable hourly rate; and
  - any other factors considered in making the award.

(*Neiman v. Naseer*, 31 So. 3d 231, 234 (Fla. 4th DCA 2010); *H.K. Dev., LLC v. Greer*, 32 So. 3d 178, 185-86 (Fla. 1st DCA 2010); *Levine v. Keaster*, 862 So. 2d 876, 881 (Fla. 4th DCA 2003).)

Criminal contempt sanctions include:

- **Fines**. When a court imposes fines for criminal contempt:
  - the fine may be a flat penalty imposed regardless of any purge conditions (*Bank of New York*, 79 So. 3d at 167);
  - the fine may not exceed $500 (§ 775.02, Fla. Stat.; *Kramer v. State*, 800 So. 2d 319, 321 (Fla. 2d DCA 2001)); and
  - the witness pays the fine to the state or into the public treasury, not to the moving party (*H.K. Dev., LLC*, 32 So. 3d at 184).
- **Imprisonment**. When a court imposes imprisonment for criminal contempt:
  - the sentence cannot exceed 12 months (§ 775.02, Fla. Stat.; *Saridakis v. State*, 936 So. 2d 33, 35 (Fla. 4th DCA 2006)); and
  - any sentence greater than six months entitles the witness to a jury trial (*Aaron v. State*, 284 So. 2d 673, 676-77 (Fla. 1973); *Forbes v. State*, 933 So. 2d 706, 714 (Fla. 4th DCA 2006)).

Enforcing a Subpoena Duces Tecum for Deposition

As with subpoenas for deposition, the issuing party seeking to enforce a subpoena *duces tecum* for deposition may file either or both a motion:

- To compel (Fla. R. Civ. P 1.410(f); and see Moving to Compel Testimony or Production of Documents).
- For contempt sanctions (Fla. R. Civ. P. 1.410(f); and see Moving for Contempt Sanctions After Non-Compliance with a Subpoena *Duces Tecum* for Deposition).

Moving to Compel Testimony or Production of Documents

Counsel may file a motion to compel testimony or the production of documents sought in a subpoena *duces tecum* for deposition when the witness:

- Fails to answer a question regarding a relevant, non-privileged matter during a deposition (Fla. R. Civ. P. 1.280(a) and 1.380(a)(2)). An evasive or incomplete answer constitutes a failure to answer a question (Fla. R. Civ. P. 1.380(a)(3)).
- Fails to designate a witness under Florida Rules of Civil Procedure 1.310(b)(6) or 1.320(a) (Fla. R. Civ. P. 1.380(a)(2)).
- Fails to appear for the deposition.
- Improperly objects or fails to produce documents or other materials sought in a subpoena *duces tecum* for deposition (Fla. R. Civ. P. 1.410(e); *Westco, Inc. v. Scott Lewis' Gardening & Trimming, Inc.*, 26 So. 3d 620, 623 (Fla. 4th DCA 2009)).
- Objects to the production of electronically stored information (ESI) as not readily accessible due to undue burden or cost (Fla. R. Civ. P. 1.410(c)).

If a witness objects to a subpoena *duces tecum* **without** deposition, filing a motion to compel is **not** the appropriate enforcement method. Counsel must first serve a subpoena *duces tecum* for deposition. (See Enforcing a Subpoena *Duces Tecum* Without Deposition.)

Where to Make the Motion

Rule 1.410(e)(1) requires counsel to file a motion to compel subpoenaed documents in the court from which counsel issued the subpoena, which typically is the court where the action is pending (Fla. R. Civ. P. 1.410(e)(1)). However, Rule 1.380 instructs counsel to file a motion to compel testimony in the court in the county where the deposition is to be taken (Fla. R. Civ. P. 1.380(a)(1)). Therefore, if a subpoenaed witness residing in a different county objects to both the document requests and the deposition, counsel may be required to file separate motions in different courts. However, in practice, counsel

typically file one motion to compel in the court where the action is pending. Counsel should be prepared to address possible venue objections at the hearing on the motion to compel. (See Enforcing a Deposition Subpoena: Moving to Compel: Where to Make the Motion.)

When to Make the Motion

As with a deposition subpoena, counsel should file a motion to compel as soon as possible after the discovery violation and before the discovery period closes (see Enforcing a Deposition Subpoena: When to Make the Motion).

Burden on the Motion

The party seeking to compel discovery has the burden of showing the discovery sought is relevant or reasonably calculated to lead to the discovery of admissible evidence (*Calderbank v. Cazares*, 435 So. 2d 377, 379 (Fla. 5th DCA 1983)).

Counsel for the moving party should address any objections made to the discovery by the witness. For information on the grounds for objecting to a subpoena, see Practice Note, Subpoenas in State Court: Responding to a Subpoena (FL): Objecting to a Document Subpoena.

Available Relief

A trial court has broad discretion in discovery matters and may issue any order it finds necessary, including entry of a protective order (Fla. R. Civ. P. 1.380(a)(2)) or an order imposing conditions on the production or compliance, such as the prepayment of the producing party's costs (Fla. R. Civ. P. 1.410(c)). The court may also award reasonable expenses, including attorneys' fees, depending on the disposition of the motion to compel (Fla. R. Civ. P. 1.380(a)(4)).

For more information on the types of relief available and the conditions for awarding fees and costs, see Enforcing a Deposition Subpoena: Available Relief.

Electronically Stored Information

On a motion to compel discovery of electronically stored information (ESI), a court has discretion to:

- Grant the motion if:
  - the witness fails to show that the ESI is not reasonably accessible because of undue cost or burden; or
  - the witness shows that the ESI is not reasonably accessible because of undue cost or burden but the requesting party still shows good cause.
- Specify conditions of the ESI discovery, such as requiring the requesting party to pay the expenses that the witness incurs.

(Fla. R. Civ. P. 1.410(c).)

The court **must** limit the frequency or extent of ESI discovery if it determines any one of the following circumstances apply:

- The discovery sought is unreasonably cumulative or duplicative.

- The discovery can be obtained from another source or in another manner that is:
  - more convenient;
  - less burdensome; or
  - less expensive.
- The burden or expense of the discovery outweighs its likely benefit considering:
  - the needs of the case;
  - the amount in controversy;
  - the parties' resources;
  - the importance of the issues at stake in the action; and
  - the importance of the discovery in resolving the issues.

(Fla. R. Civ. P. 1.280(d)(2).)

Ex Parte Motions to Compel Discovery

The issuing party may file an *ex parte* motion to compel under certain circumstances, such as when the witness fails to respond to the subpoena and does not seek an extension of time (see Enforcing a Deposition Subpoena: *Ex Parte* Motions to Compel Discovery).

Moving for Contempt Sanctions After Non-Compliance with a Subpoena Duces Tecum for Deposition

The considerations for filing a motion for contempt, including the types of contempt, the manner for filing the motion, and the available remedies, are the same as those for filing a contempt motion regarding non-compliance with a subpoena for deposition (see Moving for Contempt Sanctions After Non-Compliance with a Deposition Subpoena).

Enforcing a Subpoena Duces Tecum Without Deposition

To enforce a subpoena *duces tecum* **without** deposition (that is, a subpoena for documents only), counsel must strictly comply with Florida Rule of Civil Procedure 1.351, which differs significantly from the procedure for enforcing other types of subpoenas.

Before serving a document subpoena on the witness, the issuing party must provide all other parties in the case with notice and a copy of the subpoena to allow the parties time to object before the subpoena is served on the witness (see Practice Note, Subpoenas in State Court: Issuing and Serving a Subpoena (FL): Notice to Parties: Required Notice for Subpoenas *Duces Tecum* Without Deposition).

The method for enforcing a document subpoena depends on whether the issuing party is responding to another party's objections before service of the subpoena or the witness's objections after service of the subpoena.

Party Objections

If a party objects to a document subpoena within ten days after service of the required notice under Florida Rule of Civil Procedure 1.351, the issuing party cannot serve the subpoena and may either:

- File a motion in the issuing court to obtain a ruling on the party's objections.
- Choose not to proceed with the subpoena *duces tecum* without deposition and instead serve the witness with a subpoena *duces tecum* for deposition, which does not require advance notice to the parties.

(Fla. R. Civ. P. 1.351 (d).)

Non-Party Witness Objections

If no party objects or the court overrules the objections, the issuing party may serve the subpoena on the non-party witness. The witness may object to the subpoena any time before the deadline for compliance stated in the subpoena (Fla. R. Civ. P. 1.351(c)).

If the witness timely objects:

- The witness does not need to:
  - specify the basis for the objection; or
  - produce the evidence sought in the subpoena.
- The issuing party **cannot** seek a ruling on the objection. Instead, the issuing party must proceed under Florida Rule of Civil Procedure 1.310 and serve the witness with a subpoena *duces tecum* for deposition to learn the basis of the objection.

(Fla. R. Civ. P. 1.351(c); *Patrowicz v. Wolff*, 110 So. 3d 973, 974 (Fla. 2d DCA 2013); and see Practice Note, Subpoenas in State Court: Issuing and Serving a Subpoena (FL).)

If the witness continues to assert objections after counsel serves a subpoena *duces tecum* for deposition under Rule 1.310, counsel should enforce the subpoena by first filing a motion to compel and, if necessary, a motion for contempt (see Enforcing a Subpoena *Duces Tecum* for Deposition).

Moving for Contempt Sanctions After Non-Compliance with a Subpoena Duces Tecum Without Deposition

If the witness does not object to the subpoena and fails to produce the requested documents, counsel should consider filing a motion for contempt (Fla. R. Civ. P. 1.410(f)). The considerations for filing a motion for contempt, including the types of contempt, the manner for filing the motion, and the available remedies, are the same as those for filing a contempt motion regarding non-compliance with a subpoena for deposition (see Moving for Contempt Sanctions After Non-Compliance with a Deposition Subpoena).

Enforcing a Trial Subpoena

If a witness fails to appear in response to a trial subpoena, the subpoenaing party typically files a motion for contempt in the court from which counsel issued the subpoena (Fla. R. Civ. P. 1.410(f)). However, counsel should first take steps to attempt to ensure the witness's compliance with the trial subpoena before the trial begins to avoid unnecessary delays during trial.

Contacting the Subpoenaed Trial Witness

For most trials, counsel cannot easily predict the precise date that the case will be heard and the precise date and time that the

court will call a witness. Courts set multiple cases on the same trial docket and only hear a few of those cases during that trial period. Additional factors that may impact the trial schedule include:

- Settlement of other cases on the court's trial docket.
- The duration of other witness testimony.
- Conflicts in the court's schedule.

Counsel should include a specific date and time for compliance in a trial subpoena (Fla. R. Civ. P. 1.410(b)(1)). However, counsel also should instruct the witness in the subpoena to be available for the entire trial period to ensure the witness's availability for the subpoenaing party's case-in-chief and rebuttal.

Given this uncertainty, counsel should always remain in contact the subpoenaed witness to ensure the witness is cooperative and the witness's schedule is sufficiently flexible to permit the witness to appear whenever counsel may need to call the witness.

If counsel cannot reach the witness or the witness indicates an unwillingness to appear, counsel may choose to:

- Seek a continuance of the trial (Fla. R. Civ. P. 1.460).
- Use the witness's deposition testimony, if available, instead of live testimony at trial (Fla. R. Civ. P. 1.330(a)).
- Move for contempt if the witness does not appear at trial (Fla. R. Civ. P. 1.410(f)).

Seeking a Continuance

If counsel learns that the witness cannot appear as scheduled, counsel should consider seeking a continuance. Counsel may make the motion orally at trial or in writing before trial begins (Fla. R. Civ. P. 1.460). The motion must state the facts supporting the continuance and state when the witness is likely to be available (Fla. R. Civ. P. 1.460). The party seeking the continuance must also show that:

- Counsel acted with due diligence to obtain the witness's presence at trial.
- The witness would have provided testimony that is substantially favorable to the movant.
- The witness was available and willing to testify.
- The denial of the continuance would cause material prejudice.

(*Fisher v. Perez*, 947 So. 2d 648, 650 (Fla. 3d DCA 2007).)

Because live testimony may be more compelling to a jury, counsel should first consider seeking a continuance and take steps to obtain the witness's presence at trial. However, if counsel does not expect the witness to appear willingly, counsel should prepare to either use the witness's deposition testimony if previously taken or move for contempt sanctions if the witness fails to appear.

Using the Witness's Deposition Testimony

Alternatively, if counsel deposed the witness during discovery, counsel may consider using the witness's deposition testimony instead of live trial testimony. Although Florida subpoenas are enforceable throughout the state, if a witness is located more than 100 miles from the trial location, counsel may use the witness's deposition testimony (Fla. R. Civ. P. 1.330(a)(3)). If using deposition testimony at trial, counsel should review the court's scheduling order and ensure compliance with the deadline for designating deposition testimony, if any.

Moving for Contempt Sanctions After Non-Compliance with a Trial Subpoena

If a subpoenaed witness fails to appear at trial, counsel should request a continuance and move for contempt sanctions to compel the witness's attendance (Fla. R. Civ. P. 1.410(f)). The witness's failure to appear may constitute both indirect civil and indirect criminal contempt (see Fla. R. Civ. P. 1.410(f); *State v. Diaz de la Portilla*, 177 So. 3d 965, 973 (Fla. 2015)).

How to Make the Motion

If the witness fails to appear at trial, counsel should make an oral motion asking the court to hold the witness in contempt and impose coercive sanctions. If also requesting criminal contempt charges, counsel should move for an order to show cause why the witness should not be held in criminal contempt (Fla. R. Crim. P. 3.840).

Counsel may need to ask the court to temporarily recess or continue the trial while the contempt proceedings take place. Counsel should also request that the court issue a bench warrant or writ of bodily attachment to secure the witness's appearance at trial or the contempt hearing (*Mella v. Moskowitz*, 436 So. 2d 231, 232 (Fla. 3d DCA) cause dismissed, 443 So. 2d 980 (Fla. 1983)).

If criminal contempt sanctions are sought, the proceedings must satisfy the procedures in Fla. R. Crim. P. 3.840 (see Moving for Contempt Sanctions After Non-Compliance with a Deposition Subpoena: How to Make the Motion).

When to Make the Motion

There is no specific time for filing a motion for contempt sanctions based on disobedience with a trial subpoena. However, the witness is entitled to notice and a hearing and, if criminal contempt is charged, an opportunity to prepare a defense. Thus, the contempt proceedings may result in a significant delay in the trial proceedings. Counsel should make the motion for contempt sanctions as soon as the witness fails to appear or fails to produce the requested evidence.

Available Remedies

The court has a broad array of contempt sanctions to coerce compliance with a trial subpoena, including fines, imprisonment, an award of attorneys' fees, and other measures to punish a witness's disobedience (see Moving for Contempt Sanctions After Non-Compliance with a Deposition Subpoena: Available Remedies). In addition to these remedies, counsel should also request a writ of bodily attachment or bench warrant to secure the witness's attendance at trial (see *Mella*, 436 So. 2d at 232).

Work Product Doctrine: Basic Principles (FL)

A Practice Note analyzing the basic principles underlying the work product doctrine in Florida. Specifically, this Note covers what types of information may be protected by the work product doctrine, who may create work product, who may assert the work product protection and how long the work product protection lasts.

Contents

The work product doctrine protects documents and other materials that are generated by or for a party in preparation for litigation which reveal an attorney's mental impressions, conclusions, opinions, or legal theories from disclosure to third parties (Fla. R. Civ. P. 1.280). This Note outlines the key issues to consider in determining whether documents and other materials may properly be withheld on work product grounds.

Who can Create Work Product

The first step in analyzing whether the work product protection covers particular documents (or other materials) is to identify the document's creator. As explained below, Florida places limits on who can create work product.

Parties and Party Representatives

Work product may be created by or on behalf of a party in anticipation of litigation (*Marshalls of MA, Inc. v. Minsal*, 932 So. 2d 444, 446 (Fla. 3d DCA 2006)). Under Rule 1.280, the following persons may create work product:

- The party's attorney.
- Consultants.
- Sureties.
- Indemnitors.
- Insurers.
- Agents.

(Fla. R. Civ. P. 1.280(b)(4).)

Information created or prepared by other types of representatives of the party or the party's attorney other than those listed under Rule 1.280 may also be entitled to work product privilege. For example, courts have held that documents created by investigators and employees of a risk management department are protected from disclosure. (*Heartland Express, Inc., of Iowa v. Torres*, 90 So. 3d 365, 367-368 (Fla. 1st DCA 2012).)

The Florida courts have provided a general description of attorney work product that includes any of the following if generated by the attorney and not used as evidence:

- Views of how and when to present evidence.
- Evaluation of the importance of evidence.
- Personal knowledge of strategies for presenting witnesses.
- Personal notes as to:
  - witnesses;
  - jurors;
  - legal citations;
  - proposed arguments;
  - jury instructions; and
  - diagrams and charts.

(*Bishop ex rel. Adult Comprehensive Protective Servs., Inc. v. Polles*, 872 So. 2d 272, 274 (Fla. 2d DCA 2004).)

Other Individuals

A nonparty to the litigation can assert work product privilege (Fla. R. Civ. P. 1.280(b)(4) and *Zaban v. McCombs*, 568 So. 2d 87, 89 (Fla. 1st DCA 1990) (holding that a nonparty employer was protected by the work product privilege)).

The work product rule does not require the attorney to have ordered or requested the party or other individuals to prepare the document or materials for it to receive work product protection (*Metric Eng'g, Inc. v. Small*, 861 So. 2d 1248, 1250 (Fla. 1st DCA 2003)).

Scope of Protection

There are limits on the scope of the work product doctrine. This section of the note outlines the key issues to consider in determining the type of work product at issue, and whether particular documents (or other materials) are protected from disclosure.

Fact Work Product

Florida law differentiates between "fact" or "opinion" work product, with different degrees of protection available for each (*Acevedo v. Doctors Hosp., Inc.*, 68 So. 3d 949, 952-53 (Fla. 3d DCA 2011)).

Generally, "fact" work product includes any information that relates to the case that was gathered in anticipation of litigation, regardless of its substantive content. Fact work product is protected from disclosure unless the party seeking discovery shows a need and is unable to obtain its substantial equivalent without undue hardship. (*Heartland Express, Inc., of Iowa v. Torres*, 90 So. 3d 365, 367 (Fla. 1st DCA 2012).) For example, the following materials qualify as fact work product:

- Incident reports related to the action (*Paradise Pines Health Care Associates, LLC v. Bruce*, 27 So. 3d 83 (Fla. 1st DCA 2009)).
- Witness statements obtained by one party containing factual information related to the action (*Carnival Cruise Lines, Inc. v. Doe*, 868 So. 2d 1219 (Fla. 3d DCA 2004)).
- Statistical analysis performed by a company at the request of the company's counsel (*S. Bell Tel. & Tel. Co. v. Deason*, 632 So. 2d 1377 (Fla. 1994)).

However, the courts have held that the constitutionally guaranteed patient right to know about adverse medical incidents generally preempts any fact work product privilege that may have otherwise protected medical incident reports (Art. X, § 25(a), Fla. Const.; see also *Florida Eye Clinic, P.A. v. Gmach*, 14 So. 3d 1044, 1048-49 (Fla. 5th DCA 2009) (adverse incident reports never reviewed by counsel at time of creation held discoverable)).

Once a work product privilege is claimed, generally a court must hold an *in camera* inspection of the materials to rule on the applicability of the privilege. If the court holds that the discovery is work product, the requesting party must then prove need and undue hardship to obtain substantially equivalent information by other means to overcome the privilege. (*Town Ctr. @ Boca Raton Trust v. Hirokawa*, 789 So. 2d 1230, 1231-32 (Fla. 4th DCA 2001).)

Opinion Work Product

Opinion work product consists primarily of the mental impressions, conclusions, opinions and theories of the attorney and is generally afforded absolute immunity from disclosure (Fla. R. Civ. P. 1.280(b)(4) and see *Acevedo v. Doctors Hosp., Inc.*, 68 So. 3d 949, 953 (Fla. 3d DCA 2011)). Opinion work product includes the following examples:

- Notes taken during an interview, including attorney's conclusions related to the possible harm of interviewee's testimony (*Gen. Motors Corp. v. McGee*, 837 So. 2d 1010, 1032 (Fla. 4th DCA 2002)).
- A memo summarizing documentation relevant to the litigation (*Gen. Motors Corp. v. McGee*, 837 So. 2d 1010, 1040 (Fla. 4th DCA 2002)).

A grouping of otherwise unprotected documents made by the attorney that may reveal the attorney's theories or mental impressions has also been held by the courts to be protected work product (*Ford Motor Co. v. Hall-Edwards*, 997 So. 2d 1148, 1153 (Fla. 3d DCA 2008); but see *Northup v. Acken*, 865 So. 2d 1267, 1271 (Fla. 2004) (stating the proposition but holding the documents in that case were being used for impeachment at trial and were therefore discoverable)).

Tangible vs. Intangible

The work product protection may be extended to intangible mental impressions, personal beliefs, and the like (*Grinnell Corp. v. Palms 2100 Ocean Blvd., Ltd.*, 924 So. 2d 887, 891 (Fla. 4th DCA 2006)).

Uncommunicated Information

Uncommunicated information, such as internal memorandum, may be considered work product provided they were prepared in anticipation of litigation (see *S. Bell Tel. & Tel. Co. v. Deason*, 632 So. 2d 1377, 1384-85 (Fla. 1994)).

Facts Contained in or about Work Product Documents

Facts contained in work product documents are not protected from discovery by other means. For example, a party is permitted to discover the identity of persons having knowledge of any discoverable matter. (Fla. R. Civ. P. 1.280(b)(1).) Courts have held that the identity of persons who have furnished witness statements is discoverable by interrogatories, though the statements themselves generally will be protected work product (*Wal-Mart Stores, Inc. v. Weeks*, 696 So. 2d 855, 857 (Fla. 2d DCA 1997)).

Also, the work product doctrine does not protect facts about the creation of work product, for example the "fact" that a particular document was drafted or an interview occurred (*Grinnell Corp. v. Palms 2100 Ocean Blvd., Ltd.*, 924 So. 2d 887, 894 (Fla. 4th DCA 2006) ("Because the work product doctrine is intended only to guard against divulging the attorney's strategies and legal impressions, it does not protect facts concerning the creation of work product or facts contained within work product.")).

Experts

All materials reasonably expected or intended to be used at trial, including previous depositions by experts, are subject to discovery (*Northup v. Acken*, 865 So. 2d 1267, 1271 (Fla. 2004)). Counsel can obtain the discovery of a testifying expert's facts and opinions by using the following discovery methods:

- Interrogatories under Florida Rule of Civil Procedure 1.280(b)(5)(A) to obtain:
  - the subject matter on which the expert is expected to testify;
  - the substance of that expert's facts and opinions; and

- a summary of the grounds for each opinion.
- Depositions under Florida Rule of Civil Procedure 1.390.

However, a non-testifying expert's report, findings and opinions are protected work product (*Nevin v. Palm Beach County Sch. Bd.*, 958 So. 2d 1003, 1007 (Fla. 1st DCA 2007)). They may only be required to be produced upon a showing of exceptional circumstances or if the expert is issuing a report following an examination of a person under Florida Rule of Civil Procedure 1.360(b) (Fla. R. Civ. P. 1.280(b)(5)(B)). An expert witness later withdrawn as a testifying witness is protected under the privilege (*Rocca v. Rones*, 125 So. 3d 370, 372 (Fla. 3d DCA 2013); see also *Huet v. Tromp*, 912 So. 2d 336, 339 (Fla. 5th DCA 2005) (the inclusion of three investigators on a witness list waived the work product privilege, but the waiver was cured when an amended witness list was filed removing the three investigators from it)).

Anticipation of Litigation

The work product doctrine only protects documents (and other materials) that were prepared in anticipation of litigation or for trial (Fla. R. Civ. P. 1.280(b)(4)). The "anticipation of litigation" element generally requires courts to analyze whether the materials were created:

- In connection with "litigation."
- At a time when litigation was anticipated.
- Because of the anticipated litigation.

The First, Second, Third, and Fifth District Courts of appeal have held that the standard for "anticipation of litigation" is whether the document or materials were prepared in response to some event that could foreseeably be the basis for a claim or cause of action in the future (*Marshalls of MA, Inc. v. Minsal*, 932 So. 2d 444, 446-47 (Fla. 3d DCA 2006)). The Fourth District court, however, applies a more stringent standard of "substantial and imminent litigation (*Liberty Mut. Fire Ins. Co. v. Bennett*, 883 So. 2d 373, 374 (Fla. 4th DCA 2004) decision quashed on other grounds, 905 So. 2d 119 (Fla. 2005)).

Reports prepared both in anticipation of litigation and for prevention of subsequent accidents do not lose their work product protection because of the dual purpose where the reports were prepared after the company's legal counsel assumed oversight (*Fed. Exp. Corp. v. Cantway*, 778 So. 2d 1052, 1053-54 (Fla. 4th DCA 2001)). For example, where an incident report prepared in anticipation of litigation was distributed amongst other departments for the purpose of remedial measures, the report did not lose its work product protection (*Dist. Bd. of Trustees of Miami-Dade Cmty. Coll. v. Chao*, 739 So. 2d 105, 107 (Fla. 3d DCA 1999)).

Generally, the likelihood of litigation has been sufficient to afford work product protection under the following conditions:

- If information is prepared for dual reasons (such as incident reports prepared for personnel reasons as well as possible litigation), it will still be protected under the work product privilege if one of those reasons was for litigation (*Marshalls of MA, Inc. v. Minsal*, 932 So. 2d 444, 446 (Fla. 3d DCA 2006)).
- Incident reports for previous unrelated accidents are not discoverable in a future litigation where those reports were regularly prepared and forward to the cruise line's risk management department for use in connection with defense of any claims that may result from that incident (*Royal Caribbean Cruises, Ltd. v. Doe*, 964 So. 2d 713, 718 (Fla. 3d DCA 2007), disapproved of on other grounds by *Bd. of Trustees of Internal Improvement Trust Fund v. Am. Educ. Enters., LLC*, 99 So. 3d 450 (Fla. 2012)).
- Three years of accident reports from retailer were protected work product, even though not prepared in anticipation of that case, as they were prepared in response to some event which could foreseeably be made the basis of a claim in a future litigation (*Marshalls of MA, Inc. v. Minsal*, 932 So. 2d 444, 446-48 (Fla. 3d DCA 2006)).

An insurer's claim file is generally protected under the work product privilege prior to a determination of coverage (*State Farm Florida Ins. Co. v. Aloni*, 101 So. 3d 412, 414 (Fla. 4th DCA 2012)). However, if a first or third party bad faith claim is

filed after the resolution of the coverage dispute, the insurer's documents may be discoverable in the bad faith action (*Allstate Indem. Co. v. Ruiz*, 899 So. 2d 1121, 1129-30 (Fla. 2005)).

An attorney does not have to be the person anticipating litigation for the work-product doctrine to apply (*Orange Park Christian Acad. v. Russell*, 899 So. 2d 1215 (Fla. 1st DCA 2005) (a report produced by a teacher and the notes and memoranda prepared by the principal following a motor vehicle accident involving a student were prepared in anticipation of litigation, although no attorney was involved at that time)).

Protected work product materials retain qualified immunity from discovery even after the original litigation terminates, regardless of whether any later litigation is related (*Toward v. Cooper*, 634 So. 2d 760, 761 (Fla. 4th DCA 1994)).

The work product doctrine generally does not protect materials that were created in the ordinary course of business (*Neighborhood Health P'ship, Inc. v. Peter F. Merkle M.D., P.A.*, 8 So. 3d 1180, 1184-85 (Fla. 4th DCA 2009)).

Overcoming the Protection

The fact work product protection may be overcome if the party seeking discovery shows that it is in need of the materials in the preparation of their case and is unable without undue hardship to obtain their substantial equivalent by other means (Fla. R. Civ. P. 1.280(b)(4)). This section of the Note outlines the key issues to consider in determining whether the work product protection has been overcome in a particular instance.

Substantial Need

Work product may be discoverable if the party can show "substantial" need along with the inability to obtain the discovery by other means (*Liberty Mut. Fire Ins. Co. v. Kaufman*, 885 So. 2d 905, 910 (Fla. 3d DCA 2004)). To demonstrate the need, the requesting party must present evidence or testimony that demonstrates that the requested material is critical to the theory of the requesting party's case, or some significant portion of their case (*Zirkelbach Constr., Inc. v. Rajan*, 93 So. 3d 1124, 1129-30 (Fla. 2d DCA 2012)).

Where the normal tools of discovery are insufficient to obtain the facts in otherwise protected work product and those facts are relevant to the claim, the requesting party has shown a need (*Dist. Bd. of Trustees of Miami-Dade Cmty. Coll. v. Chao*, 739 So. 2d 105, 107 (Fla. 3d DCA 1999)).

Courts have held that requests for work product protected discovery for the purpose of comparing or identifying inconsistencies in investigations, especially if the other party has hired or could hire their own expert, do not create a sufficient showing of need (*Nevin v. Palm Beach County Sch. Bd.*, 958 So. 2d 1003, 1006-07 (Fla. 1st DCA 2007)). Inconsistencies in testimony are also not a sufficient need to compel production of work product materials (*Florida Farm Bureau Gen. Ins. Co. v. Copertino*, 810 So. 2d 1076, 1080 (Fla. 4th DCA 2002)).

Undue Hardship

Undue hardship is often fact dependent and combined with the substantial equivalent and need requirements when considered by the courts. However, to overcome a work product protection, the showing of undue hardship must be more than a bare assertion and must include specific explanations and reasons. (*Ashemimry v. Ba Nafa*, 847 So. 2d 603, 605 (Fla. 5th DCA 2003).) The showing must be made by affidavit or sworn testimony (*Falco v. N. Shore Labs. Corp.*, 866 So. 2d 1255, 1257 (Fla. 1st DCA 2004)).

The following circumstances have been held to meet the undue hardship requirement necessary to compel production of work product:

- When the party asserting privilege over work product is not forthcoming in disclosing individuals named in an incident report (*Dist. Bd. of Trustees of Miami-Dade Cmty. Coll. v. Chao*, 739 So. 2d 105, 107-08 (Fla. 3d DCA 1999)).
- Where the underlying data consisted of over 1,000,000 trouble repair reports, the court found that the task of analyzing that information to obtain the equivalent of an investigative audit was unduly arduous and unrealistic and precisely the kind of undue hardship contemplated by Rule 1.280(b)(4) (*S. Bell Tel. & Tel. Co. v. Deason*, 632 So. 2d 1377, 1385 (Fla. 1994)).
- When relevant witnesses are no longer available or can only be contacted with great difficulty (*Dist. Bd. of Trustees of Miami-Dade Cmty. Coll. v. Chao*, 739 So. 2d 105, 107 (Fla. 3d DCA 1999)).

Substantial Equivalent

The courts have not established a clear legal standard to determine whether evidence is "substantial equivalent." Instead, an evidentiary hearing is required to determine whether the substantial equivalent of the requested discovery could be obtained by other means. (See *Florida E. Coast Ry., L.L.C. v. Jones*, 847 So. 2d 1118, 1119 (Fla. 1st DCA 2003).)

Generally, however, where a requesting party could obtain the substantial equivalent of the information or materials through the ordinary tools of discovery, work product protected discovery cannot be compelled (*Universal City Dev. Partners, Ltd. v. Pupillo*, 54 So. 3d 612, 614 (Fla. 5th DCA 2011)). Examples where the courts have found that the "substantial equivalent" standard has been met include the following:

- Party who had already deposed one witness and knew of other witnesses, but had not deposed them, was able to obtain the substantial equivalent of witness statements without undue hardship (*Carnival Cruise Lines, Inc. v. Doe*, 868 So. 2d 1219, 1221 (Fla. 3d DCA 2004)).
- Party was able to obtain facts of an alleged battery through interrogatories and depositions instead of requiring the production of the alleged battery incident report which was work product (*Universal City Dev. Partners, Ltd. v. Pupillo*, 54 So. 3d 612, 614 (Fla. 5th DCA 2011)).

Effect on Opinion Work Product

While factual work product is subject to discovery upon a showing of need and undue hardship, opinion work product generally remains protected from disclosure (*Acevedo v. Doctors Hosp., Inc.*, 68 So. 3d 949, 953 (Fla. 3d DCA 2011) (opinion work product generally receives "absolute immunity")).

Waiver

Although Florida does not favor waiver of work product privileges (see *Coates v. Akerman, Senterfitt & Eidson, P.A.*, 940 So. 2d 504, 508 (Fla. 2d DCA 2006)), the work product protection may later be waived by a party's conduct. This section of the Note outlines the key issues to consider in determining whether the work product protection has potentially been waived.

Who can Waive

The work product protection, unlike the attorney-client privilege, can protect both the client and the attorney and can be asserted by either (*State v. Rabin*, 495 So. 2d 257, 262 n.8 (Fla. 3d DCA 1986)). A client may waive fact work product protection because an attorney has no significant interest in such materials. But an attorney sometimes has a significant privacy interest in opinion work product, so the attorney's opinion work product may remain protected from disclosure. (*State v. Rabin*, 495 So. 2d 257, 263-64 (Fla. 3d DCA 1986).) Although rare, a nonparty may also invoke the privilege (*Zaban v. McCombs*, 568 So. 2d 87, 89 (Fla. 1st DCA 1990)).

Disclosures between clients with a common interest in litigation generally does not waive the work product privilege. Waiver of an attorney-client privilege also does not constitute an automatic waiver of the work product privilege. (*Visual Scene, Inc. v. Pilkington Bros., plc.*, 508 So. 2d 437, 442 (Fla. 3d DCA 1987).)

Express Waiver

A party may expressly waive the work product protection by disclosing work product to certain third parties. This section of the note identifies the types of disclosures that may (and may not) waive the work product protection.

Intentional Disclosure

When a party intentionally discloses material that is privileged, any privilege is expressly waived (§ 90.507, Fla. Stat.; *St. Paul Fire & Marine Ins. Co. v. Welsh*, 501 So. 2d 54, 57 (Fla. 4th DCA 1987)).

Unintentional Disclosure

Fla. R. Civ. P. 1.285 protects a party against the inadvertent disclosure of materials that are privileged. Within 10 days of discovering the inadvertent disclosure, the disclosing party must serve written notice of the privilege upon the party to whom the materials were disclosed. The written notice must describe with particularity:

- The materials for which the privilege is asserted.
- The nature of the privilege.
- The date the inadvertent disclosure was discovered.

(Fla. R. Civ. P. 1.285(a).)

The party receiving the notice must:

- Promptly return, sequester or destroy the materials and all copies subject to the privilege claim.
- Notify any other person, party or entity to whom it has disclosed the materials of the notice.
- Take reasonable steps to recover any materials disclosed to others.

(Fla. R. Civ. P. 1.285(b).)

The party receiving the notice may challenge the assertion of the privilege based upon any of the following (as well as other grounds):

- The materials are not privileged.
- The person asserting the privilege lacks standing to do so.
- The disclosing party has failed to timely serve the notice.

- The privilege has been waived.

(Fla. R. Civ. P. 1.285(c).)

Otherwise, a party's unintentional disclosure of a protected document may waive the work product doctrine.

The courts typically employ a five-part test to determine if the disclosure was inadvertently waived and whether or not protection remains:

- The precautions taken to prevent the disclosure and the reasonableness of them.
- The number of disclosures made.
- The extent of the disclosure made.
- Timeliness and the measures taken to rectify the disclosure.
- Would the overriding interests of justice be served by maintaining the protection.

(*Gen. Motors Corp. v. McGee*, 837 So. 2d 1010, 1040 (Fla. 4th DCA 2002).)

Failure by a party to assert a work product privilege at the earliest opportunity does not result in an automatic waiver of that privilege, as long as the privilege is asserted before the protected information has been disclosed (*Truly Nolen Exterminating, Inc. v. Thomasson*, 554 So. 2d 5, 5-6 (Fla. 3d DCA 1989)).

Selective Waiver

Disclosure to one adversarial party, such as the government, may operate as a waiver of the work product protection unless the disclosing party can show that the disclosure was compelled, such as through a subpoena (*Carnival Cruise Lines, Inc. v. Doe*, 868 So. 2d 1219, 1221 (Fla. 3d DCA 2004)).

A party may also make a limited waiver of the work product privilege (*Paradise Divers, Inc. v. Upmal*, 943 So. 2d 812, 814 (Fla. 3d DCA 2006) (party's disclosure of portions of its attorney's file relevant to its advice of counsel defense on one count of the complaint did not waive the work product privilege as to investigative materials, mental impressions or communications concerning other counts of the complaint)).

Disclosure of Facts

A party does not normally waive the work product protection by merely disclosing facts. Facts of a case and the documents and materials that are part of those facts are not protected work product, as distinguished from materials prepared in preparation for litigation and the attorney's evaluation of items produced in discovery to create a litigation strategy. As a result, there is no privilege to waive. (*Grinnell Corp. v. Palms 2100 Ocean Blvd., Ltd.*, 924 So. 2d 887, 892-94 (Fla. 4th DCA 2006).)

Compelled Disclosure

If a court erroneously compels disclosure of protected work product, the involuntary disclosure does not waive the work product privilege (§ 90.508, Fla. Stat.).

Waiver as Litigation Sanction

The courts in Florida generally disfavor finding an implicit waiver of work product protection as a sanction for a discovery violation and reserves it only for serious violations (*Bankers Sec. Ins. Co. v. Symons*, 889 So.2d 93, 95 (Fla. 5th DCA 2004)). When a party fails to provide a privilege log under Florida Rule of Civil Procedure 1.280(b)(6) for information otherwise discoverable, the courts have held that the sanction may be warranted depending on the conduct of the party asserting the protection. A Florida court found a waiver of work product protection where the party did not file a privilege log and did not claim the protection until trial, disrupting the trial. (*Gen. Motors Corp. v. McGee*, 837 So. 2d 1010, 1032-33 (Fla. 4th DCA 2002)). However, if a party fails to submit a privilege log by the required due date, it does not operate as an automatic waiver of a work product privilege (*Bankers Sec. Ins. Co. v. Symons*, 889 So. 2d 93, 95 (Fla. 5th DCA 2004)).

Also, a privilege log is not required where the work product privilege claimed is category specific and not document specific. For example, where a party claimed a categorical work product privilege for their non-testifying expert, failure to produce a privilege log did not waive the protection as a privilege log was not required. (*Nevin v. Palm Beach County Sch. Bd.*, 958 So. 2d 1003, 1008 (Fla. 1st DCA 2007).)

Subpoenas in State Court: Obtaining Out-of-State Discovery (FL)

A Practice Note explaining how to obtain non-party discovery outside of Florida for an action pending in Florida state court. This Note addresses how to comply with Florida law before seeking discovery outside of Florida, how to comply with the law of a different US state, including compliance with the Uniform Interstate Deposition and Discovery Act (UIDDA), the Uniform Foreign Depositions Act (UFDA), or a state's non-uniform law, and how to handle post-service procedures, including enforcing an out-of-state subpoena.

Contents

During litigation, parties may need to subpoena documents or deposition testimony from a non-party located in another state. The procedures for issuing and serving a subpoena vary depending on the type of discovery sought and the state in which the witness or documents are located. If seeking discovery outside of Florida but within the US, counsel may need to comply with the Uniform Interstate Deposition and Discovery Act (UIDDA), the Uniform Foreign Depositions Act (UFDA), or a

non-uniform state procedure. This Note explains how Florida counsel can seek discovery from a non-party outside of Florida according to Florida law and the law of the target state.

Comply with Florida Law

To obtain non-party discovery in another state for a case pending in Florida, counsel must first comply with certain procedural requirements under Florida law, unless the non-party has agreed to voluntarily provide the discovery.

Document Subpoenas

Counsels' first step in seeking documents from a non-party witness **without** a deposition is the same regardless of whether the non-party witness resides in Florida or outside of Florida. Specifically, counsel must serve a Notice of Intent to Serve Subpoena *Duces Tecum* Without Deposition on all parties, wait ten days to allow any party to object, and resolve any objections **before** issuing the subpoena. (Fla. R. Civ. P. 1.351; see Practice Note, Subpoenas in State Court: Issuing and Serving a Subpoena (FL): Notice to Parties: Required Notice for Subpoena Duces Tecum Without Deposition.)

Florida law does not require parties to seek a court order permitting the document discovery, except to resolve any objections raised by the other parties. Once an attorney sends the required notice, waits ten days, and resolves any objections, the next step is to comply with the law of the state where the witness is located (see Comply with the Law of the Target State).

Deposition Subpoenas

A party seeking an out-of-state deposition, whether with or without a request for documents, must first obtain an order from the Florida court appointing an out-of-state notary (or other qualified individual) to administer the oath and transcribe the deposition testimony (Fla. R. Civ. P. 1.300(a)). This person is referred to as a "commissioner," and is typically the court reporter who transcribes the deposition (most court reporters are also notaries).

To obtain the Florida court order appointing a commissioner, counsel should:

- Identify a court reporter authorized to administer oaths and take depositions under the law of the target state (that is, the state where counsel seek discovery).
- Draft a short Motion to Appoint Commissioner to Take Out-of-State Deposition. The motion should:
  - briefly explain why counsel require the deposition of the out-of-state witness;
  - identify the name and qualifications of the court reporter;
  - request that the court appoint the court reporter as a commissioner authorized to take the deposition in the target state; and
  - request that the court authorize the moving party to serve a subpoena in the target state to compel the witness's testimony before the court reporter.
- Draft a proposed Order Appointing Commissioner and Authorizing Out-of-State Deposition. The proposed order should:
  - appoint the court reporter as a commissioner authorized to take the deposition of the witness;
  - authorize the requesting party to serve a subpoena in the target state to compel the witness's testimony; and
  - state that the subpoena must be served, and the deposition must be taken, under the law of the target state, citing the target state's law (see Interstate Discovery Chart).
- Send a copy of the motion and proposed order to the parties in the case and ask whether they oppose the relief requested. Parties rarely object to the appointment of a commissioner. Counsel should title the motion "Unopposed" if

no party objects.
- File and serve the motion, with the proposed order attached, and set it for a **motion calendar hearing** (see Practice Note, Motion Practice: Service and Filing (FL)).
- Attend the hearing and obtain the executed order.

After obtaining an executed order, counsel should:

- Deliver a copy to the court reporter whom the court appointed as a commissioner.
- File a Notice of Deposition and serve it on all parties to the Florida action (Fla. R. Civ. P. 1.410(e)(1); see Standard Document, Notice of Deposition (FL)).

Once counsel complete these steps, they must have the subpoena issued and served following the law of the target state.

Comply with the Law of the Target State

After taking all necessary steps under Florida law to secure the desired out-of-state non-party discovery, counsel must look to the law of the target state to complete the discovery process.

UIDDA Jurisdictions

Most states have enacted a version of the UIDDA (for the full list, see Interstate Discovery Chart). When seeking discovery in a jurisdiction that has enacted the UIDDA, counsel should:

- Check if the target state's version of the UIDDA requires reciprocal treatment from Florida (see Check If the Target State Requires Reciprocity).
- Check if the target state also offers non-uniform procedures that may be more appropriate for the particular case (see Check If the Target State Also Has Non-UIDDA Procedures).
- Issue and serve a subpoena that complies with the target state's version of the UIDDA and local practice (see Issue a Subpoena Under the UIDDA and Serve a Subpoena Under the UIDDA).

Check If the Target State Requires Reciprocity

Some states do not permit an out-of-state litigant to use that state's UIDDA unless the state where the action is pending has adopted the UIDDA or a similar law. Florida has not adopted the UIDDA. Counsel must therefore check if the target state has a reciprocity requirement and, if so, whether its reciprocity requirement is nevertheless broad enough to allow a Florida litigant to use the target state's UIDDA. For example:

- Virginia's reciprocity requirement extends to any state that has enacted the UIDDA, a predecessor uniform act, or any other comparable law (Va. Code Ann. § 8.01-412.14). Virginia effectively extends its UIDDA procedures to Florida litigants, as Florida has adopted a predecessor uniform act (the UFDA).
- Georgia's reciprocity requirement only extends to other states that have enacted the UIDDA (O.C.G.A. § 24-13-112(d)). Georgia law therefore precludes Florida litigants from seeking discovery under its version of the UIDDA.

If the target state's reciprocity requirement effectively prohibits Florida litigants from seeking discovery under its version of the UIDDA, counsel must review the state's alternative out-of-state discovery procedures (for example, O.C.G.A. §§ 24-13-110 to 24-13-116 (alternative procedures for out-of-state litigants to obtain non-party discovery in Georgia)).

For information on which states require reciprocity, see Interstate Discovery Chart.

Check If the Target State Also Has Non-UIDDA Procedures
Several states have both the UIDDA and an alternative non-uniform procedure. If there is an alternative procedure, counsel should determine whether that procedure is more appropriate based on the circumstances.

Although the UIDDA is typically more cost-effective and expeditious, other procedures may have different benefits. For example, under Alabama's non-uniform procedure, an Alabama judge issues the subpoena (Ala. R. Civ. P. 28(c)). This procedure may require more time and expense up front, but could be a better approach if counsel anticipate an uncooperative witness. A witness may be more likely to comply with a judge-ordered subpoena than one that is issued by a court clerk under Alabama's version of the UIDDA (see Ala. Code § 12-21-402(b)).

For more information on which states have both the UIDDA and an alternative non-uniform procedure, see Interstate Discovery Chart.

Issue a Subpoena Under the UIDDA
If the target state's version of the UIDDA permits Florida litigants to seek discovery within its borders, Florida counsel must prepare a subpoena to be issued and served within the target state.

To issue a subpoena under the UIDDA, Florida counsel must:

- Draft and sign a Florida subpoena.
- Depending on the target state's version of the UIDDA, present the Florida subpoena to either:
  - the appropriate clerk of court (as identified in the UIDDA) in the county where discovery is sought; or
  - an attorney admitted to practice law in the target state.

After receiving the Florida subpoena, the clerk (or attorney, if permitted) must issue an identical subpoena following the target state's procedures directed to the person or entity identified in the Florida subpoena. The subpoena issued by the clerk (or attorney) of the target state must incorporate:

- The terms of the Florida subpoena, including the date, time, and place of the deposition, if seeking testimony.
- The names, addresses, and phone numbers of all counsel of record and any unrepresented party in the Florida action.
- Any additional information required by the target state's version of the UIDDA. For example, Arizona requires a subpoena issued under its UIDDA to contain the out-of-state lawsuit's caption and case number (Ariz. R. Civ. P. 45.1).

Keep the following points in mind when issuing a subpoena under the UIDDA:

- **Court clerk vs. local counsel.** Some states give parties the option to have either a court clerk or a local attorney in the target state issue the subpoena (for example, CPLR 3119(b); Cal. Civ. Proc. Code § 2029.350(a)). In these states, counsel should weigh the costs and benefits of having:
  - a local attorney issue the subpoena, which may be more expensive but may be faster and provide the opportunity for the attorney to advise Florida counsel on local practice; or
  - a clerk issue the subpoena, which may make the witness more inclined to obey the subpoena than if it were issued by an attorney.
- **Who drafts the subpoena?** In some states, the clerk or attorney in the target state drafts the subpoena, and in other states, out-of-state counsel prepare the subpoena in the appropriate form for the clerk's or local attorney's signature.
- **Where should the subpoena be issued from?** The subpoena must be issued from the county in the target state where

counsel seek the discovery (for example, 735 ILCS 35/3). Counsel should therefore ensure that the caption of the target state's subpoena identifies the court in the county where counsel seek the discovery (usually where the witness lives or works). If the subpoena is being issued by:

- a court clerk, counsel should ensure that the clerk is from the court named in the caption; or
- a local attorney, counsel need not retain an attorney in the county where the discovery is sought, but the caption of the subpoena must still identify the appropriate court.

- **Additional documents and fees.** Before requesting a court clerk to issue a subpoena, check whether the target state requires counsel to submit additional forms with the out-of-state subpoena and pay the clerk certain fees (for example, Cal. Civ. Proc. Code § 2029.300(b)(1), (2)).
- **Court appearance.** Having the target state issue a subpoena does not constitute a court appearance under the UIDDA (for example, Md. Code Ann., Cts. & Jud. Proc. § 9-402). Local counsel is therefore not required for this step in the process.

Serve a Subpoena Under the UIDDA

After obtaining the out-of-state subpoena, counsel must arrange to serve the witness. The UIDDA provides that service on the witness must comply with the target state's laws on service of process (for example, La. R.S. 13:3825(D)). Counsel should review the target state's laws or consult a licensed attorney to assist with serving the witness, particularly if counsel anticipate that the witness may attempt to evade service.

Although the UIDDA requires that service comply with the target state's law, Section 48.194, Florida Statutes requires that out-of-state subpoena service also comply with **Florida's** service of process rules (specifically, §§ 48.011 through 48.31, Fla. Stat. (Florida's service of process rules)). For example, even if service complied with the target state's law, a Florida court may invalidate service if the process server did not provide an affidavit of service containing all the details required by Florida law (see *SDS-IC v. Fla. Concentrates Int'l, LLC*, 157 So. 3d 389, 391-92 (Fla. 2d DCA 2015)).

Before attempting service, Florida counsel should therefore consult with the process server to ensure that the particulars of service comply with both Florida law and the law of the target state. For example:

- **Who may serve.** Under Florida law, a sheriff or licensed process server may serve a subpoena (§ 48.021(1), Fla. Stat.). Check which individuals may serve subpoenas under the laws of the target state as well.
- **Who may accept service.** Florida law identifies specific individuals who may accept service on behalf of the witness. For example, certain corporate officers may accept service on behalf of a corporation (§ 48.081, Fla. Stat.; see also § 48.061, Fla. Stat. (partnership); § 655.0201, Fla. Stat. (financial institution); § 48.041, Fla. Stat. (minor)). Check who may accept service of a subpoena under the laws of the target state as well.
- **What to serve.** Under Florida law, counsel must serve the witness with the subpoena and a check for attendance and mileage fees (§§ 92.142(1) and 92.151, Fla. Stat.). Check whether the target state requires that counsel:
  - pay any other (or greater) compensation to the witness; or
  - serve the witness with any documents in addition to the subpoena.
- **When to serve.** Florida law prohibits service of process on a Sunday. If a party serves a subpoena on a Sunday without a court order permitting it, the service is void and the party may be liable for damages. (§ 48.20, Fla. Stat.)
- **Methods of service.** Under Florida law, service is made by hand-delivering a copy of the subpoena directly to the witness or leaving it at the witness's residence with a person 15 years or older that resides there (§ 48.031(1), Fla. Stat.; see also § 48.031(2), Fla. Stat. (methods for substitute service)). Service can be made on a corporation by hand-delivery to the registered agent between 10 a.m. and 12 p.m. on work days (§§ 48.081(3)(a) and 48.091(2), Fla. Stat.). Check whether the target state's law provides for a similar method of service.

The UIDDA only requires service of the out-of-state subpoena. However, if taking a deposition, counsel should also serve the witness with the Florida court's Order Appointing Commissioner (see Deposition Subpoenas). Florida law does not require serving the court order with the subpoena, but doing so:

- Informs the witness that the Florida court previously authorized the deposition.
- Reduces the risk that the witness will refuse to comply.

UFDA Jurisdictions

The UFDA is a predecessor uniform law to the UIDDA. Under the UFDA, counsel **must seek a deposition**, either with or without the production of documents. The UFDA does not provide a method for serving a subpoena for documents without deposition. (*Quest Diagnostics Inc. v. Swaters*, 94 So. 3d 635, 640 (Fla. 4th DCA 2012).) However, after the subpoena is served, counsel can advise the witness that a deposition is unnecessary if the witness provides counsel with the requested documents.

When seeking discovery in a jurisdiction that has enacted the UFDA, counsel should:

- Check if the target state offers the UIDDA as an alternative method to obtain the discovery and, if so, whether that method is preferable (see Check If the Target State Has Adopted the UIDDA).
- Obtain an order from the Florida court that appoints a commissioner and authorizes an out-of-state deposition (see Obtain an Order Appointing a Commissioner from the Florida Court).
- Issue and serve a subpoena that complies with the target state's version of the UFDA and local practice (see Issue and Serve a Subpoena Under the UFDA).

Check If the Target State Has Adopted the UIDDA

Seven states offer the UFDA as a means to obtain out-of-state discovery. Some of these states require the UFDA exclusively, while others have both the UFDA and UIDDA.

The UFDA is the exclusive procedure in:

- Florida (Fla. Stat. § 92.251).
- New Hampshire (N.H. RSA § 517:18).
- Wyoming (Wyo. Stat. Ann. § 1-12-115).

The UFDA is an authorized procedure for obtaining out-of-state discovery in addition to the UIDDA in:

- Georgia (O.C.G.A. § 24-13-113). Note that Georgia's UIDDA requires reciprocity (O.C.G.A. § 24-13-112(d)).
- Louisiana (La. R.S. 13:3821).
- New York (CPLR 3102(e)).
- South Dakota (SDCL § 19-5-4).

The UFDA typically requires more court involvement than the UIDDA for issuance of a subpoena. For example, because the UFDA authorizes only deposition subpoenas, Florida counsel must obtain an order from the Florida court appointing a commissioner before issuing a subpoena (see Deposition Subpoenas). Moreover, in some target-states, such as New York, counsel typically must obtain a court order to compel a witness's attendance under the UFDA (for example, CPLR 3102(e) ("The supreme court or a county court shall make any appropriate order in aid of taking such a deposition.")). Counsel therefore may prefer to use the UIDDA where available.

For a list of all states and their out-of-state discovery procedures, see Interstate Discovery Chart.

Obtain an Order Appointing Commissioner from the Florida Court

The UFDA permits counsel to compel a deposition in the target state under the same methods as any compelled non-party deposition in that state after counsel obtain a mandate, writ, or commission from the court where the action is pending. Some states permit the deposition without a mandate, writ, or commission if the parties agree to the deposition. However, Florida law requires a commission whenever counsel seek an out-of-state deposition (which, again, is the only type of discovery allowed under the UFDA), regardless of whether the target state also requires it. For information explaining how to obtain a court order appointing a commissioner, see Deposition Subpoenas.

Issue and Serve a Subpoena Under the UFDA

The UFDA does not provide specific guidance on issuing and serving a subpoena. Instead, the UFDA typically provides that counsel may compel a witness's deposition in the same manner and by the same process as in the target state (for example, Wyo. Stat. Ann. § 1-12-115). Given the UFDA's deference to state procedure, counsel will likely benefit from retaining local counsel familiar with state law and local practice. Nevertheless, the procedure will likely require counsel to:

- Present the Florida court's Order Appointing Commissioner to the proper authority that can issue a subpoena in the target state, which is:
  - a licensed attorney in most states; or
  - a court clerk if seeking discovery in Georgia (O.C.G.A. § 24-13-113(b)).
- Ask the attorney or clerk to issue a **deposition subpoena** that complies with local practice and the law of the target state. Counsel should provide the attorney or clerk with the details of the deposition (for example, the witness's name and the location of the deposition).
- Check that the deposition subpoena contains all the necessary terms to ensure compliance by the witness, including:
  - the date, time, and place of the deposition; and
  - an attached list of documents to produce, if applicable.
- Retain a process server to serve the subpoena on the witness under the law governing service of process in the target state. The process server should also serve the witness with the Florida court's Order Appointing Commissioner. Neither Florida law nor the UFDA requires that counsel serve the court order with the subpoena, but doing so:
  - informs the witness that the Florida court previously authorized the deposition; and
  - reduces the risk that the witness will refuse to comply.

Although the UFDA requires that service comply with the target state's law, Section 48.194, Florida Statutes requires that out-of-state subpoena service also comply with **Florida's** service of process rules (specifically, §§ 48.011 through 48.31, Fla. Stat. (Florida's service of process rules)). For a discussion of the issues counsel must consider to ensure compliance with both Florida's and the target state's service of process rules, see Serve a Subpoena Under the UIDDA.

Jurisdictions with Non-Uniform Procedures

Some jurisdictions offer a non-uniform procedure for obtaining out-of-state discovery. That is, the state offers a procedure that is neither the UIDDA nor the UFDA but instead a procedure unique to that state. When seeking discovery in a jurisdiction that has a non-uniform procedure, counsel should:

- Check if the non-uniform procedure is the exclusive method or if the target state offers the UIDDA as an alternative method to obtain the discovery (see Check If the Non-Uniform Procedure is the Exclusive Method).
- Obtain an order appointing a commissioner if seeking an out-of-state deposition (see Obtain an Order Appointing a Commissioner If Seeking a Deposition).
- Issue and serve a subpoena that complies with the target state's non-uniform procedure (see Issue and Serve a Subpoena Under a Non-Uniform Procedure).

Check If the Non-Uniform Procedure is the Exclusive Method

Twenty-two states offer a non-uniform procedure for obtaining out-of-state discovery. Some of these states require the non-uniform procedure exclusively, while others offer both the non-uniform procedure and the UIDDA as acceptable means to obtain discovery. No state offers a non-uniform procedure and the UFDA.

The non-uniform procedure is the **exclusive** procedure for obtaining out-of-state discovery in:

- Arkansas (Ark. R. Civ. P. 45(f)).
- Connecticut (Conn. Gen. Stat. Ann. § 52-148e(f)).
- Maine (Me. R. Civ. P. 30(h)).
- Massachusetts (M.G.L. ch. 233, § 45).
- Missouri (Mo. Sup. Ct. R. 57.08).
- Nebraska (Neb. Ct. R. Disc. § 6-328(e)).
- Oklahoma (Okla. Stat. tit. 12, § 2004.1(A)(2)(a)).
- Rhode Island (R.I. Gen. Laws § 9-18-11).
- Texas (Tex. Civ. Prac. & Rem. Code Ann. § 20.002).

The remaining 13 states that have a non-uniform procedure also offer the UIDDA as an alternative. For the complete list, see Interstate Discovery Chart.

If seeking discovery in one of these 13 states, counsel should review both:

- The UIDDA procedure (see *UIDDA Jurisdictions*).
- The state's non-uniform procedure.

Depending on the circumstances of the case, counsel may prefer the UIDDA over the non-uniform procedure or vice versa. For example, if counsel:

- Anticipate needing to take measures to enforce the subpoena against an uncooperative witness, counsel may prefer the non-uniform procedure of some states, many of which require that counsel file a formal miscellaneous action and seek a court-issued subpoena (for example, Me. R. Civ. P. 30(h)).
- Do not anticipate an uncooperative witness, counsel may prefer the relative ease with which subpoenas are issued under the UIDDA, where a clerk or attorney, not the court, issues the subpoena.

Obtain an Order Appointing Commissioner If Seeking a Deposition

Florida law requires that a party obtain an order from the Florida court appointing a commissioner to take a deposition outside of Florida. Therefore, even if the law of the target state's non-uniform procedure does not require it, counsel must first obtain the Florida court order before issuing and serving an out-of-state deposition subpoena. If counsel seek only documents, Florida law does not require a court order. For information explaining how to obtain a court order appointing a commissioner, see Deposition Subpoenas.

Issue and Serve a Subpoena Under a Non-Uniform Procedure

The process for issuing and serving a subpoena in a state without a uniform procedure varies widely from state to state. For example, the non-uniform procedure could involve:

- Presenting to the clerk a notice of deposition prepared and served in the Florida action (Ark. R. Civ. P. 45(f)).

- Opening an action and filing an application for issuance of the subpoena (Me. R. Civ. P. 30(h)).
- Obtaining a commission from the Florida court and compelling the deposition without involving the court clerk or the court (Tex. Civ. Prac. & Rem. Code Ann. § 20.002).
- Filing a notice of deposition and request for subpoena in the court where the deposition will take place (Utah R. Civ. P. 45(a)).

Counsel must consult the state's procedural rules for the specific requirements governing both issuing and serving a subpoena. Even if not required, counsel should consider retaining local counsel to ensure the appropriate procedure is followed, particularly if the rules are unclear or counsel anticipate the witness will be uncooperative.

The target state's procedural rules typically require service of a subpoena in compliance with the target state's service of process rules. However, Section 48.194, Florida Statutes requires that out-of-state subpoena service also comply with **Florida's** service of process rules (§§ 48.011 to 48.31, Fla. Stat.). For a discussion of the issues counsel must consider to ensure compliance with both Florida's and the target state's service of process rules, see Serve a Subpoena Under the UIDDA.

Post-Service Procedure and Enforcement

After serving the subpoena, counsel for the party seeking discovery must:

- File an affidavit of service in the Florida court (see File the Affidavit of Service).
- Ensure the discovery is taken in a manner consistent with the target state's law (see Check the Rules for Taking Discovery in the Target State).
- Consider the measures counsel may need to take to enforce the subpoena or defend against a challenge to the subpoena (see Consider Measures to Enforce or Challenge the Subpoena).

File the Affidavit of Service

After serving the out-of-state subpoena on the witness, Florida counsel must obtain an affidavit of service from the process server identifying:

- The time of service.
- The manner of service (for example, in-hand or substitute service).
- The location of service.

(§ 48.194(1), Fla. Stat.)

Florida law requires that counsel file the affidavit of service in the Florida court. If another party challenges service, the court will likely consider the affidavit to determine whether service was proper. (§ 48.194(1), Fla. Stat.) If counsel anticipate a challenge, counsel should ask the process server to provide as much detail as possible in the affidavit.

Check the Rules for Taking Discovery in the Target State

Regardless of whether a party seeks discovery under the UIDDA, the UFDA, or a non-uniform procedure, any deposition or document production taking place in the target state must comply with the rules of civil procedure of that state (for example, Cal. Civ. Proc. Code § 2029.500 (UIDDA); CPLR 3102(e) (UFDA); Ark. R. Civ. P. 45(f) (non-uniform procedure)). Florida rules of civil procedure do not apply to the methods for examining an out-of-state witness or arranging for the production of documents outside of Florida. Therefore, counsel should review the target state's rules of civil procedure and consider, for example:

- Any limitations on:
  - the location of a deposition or document production (for example, only in the county where the witness resides or documents are located);
  - the duration of a deposition; or
  - the number of document requests a party may make.
- The types of valid objections counsel may make during a deposition.
- How the non-party is permitted to produce documents (for example, separated by document request or as the documents are kept in the ordinary course of business).

Consider Measures to Enforce or Challenge the Subpoena

If the out-of-state witness objects to the subpoena or fails to fully comply, Florida counsel may need to take measures to enforce the subpoena. These measures may include, for example, a motion:

- To compel compliance.
- For sanctions or contempt.
- To overrule objections.

The witness may take preemptive court action to avoid compliance with the subpoena. These measures may include, for example, a motion:

- For a protective order.
- To modify the subpoena.
- To quash the subpoena.

Regardless of whether the relief is sought by the party seeking discovery or the witness, the court in the jurisdiction where counsel served the subpoena has the **exclusive** authority to enforce the subpoena (see *Yelp, Inc. v. Hadeed Carpet Cleaning, Inc.*, 770 S.E.2d 440, 444 (Va. 2015) (citing cases)). Florida law considers the proceeding in the target state as a separate but ancillary action to the underlying Florida case (see *Freedom Newspapers, Inc. v. Egly*, 507 So. 2d 1180, 1183 (Fla. 2d DCA 1987)).

The measures taken to either enforce or challenge the subpoena in the target state must comply with the law of the target state (for example, D.C. Code § 13-446 (UIDDA); La. R.S. 13:3821 (UFDA); M.G.L. ch. 223A, § 11 (non-uniform procedure)). That is, any motion must comply with the target state's procedural and evidentiary rules. Therefore, whether defending against a challenge or attempting to enforce the subpoena, Florida counsel should retain local counsel familiar with the target state's practice and procedure. Florida counsel also typically need local counsel to file motions or appear in court.

If Florida counsel anticipate needing to take enforcement measures, counsel should consider acting in advance to deter a reluctant witness from ignoring the subpoena, for example, by:

- Obtaining an order from the Florida court authorizing the discovery and serving the witness with the court order. If seeking a deposition out-of-state, this Florida court order is required anyway (see Deposition Subpoenas).
- Retaining local counsel to serve the subpoena. Counsel should inform the witness that the party seeking discovery has retained local counsel to handle any objections or take enforcement actions, if necessary.
- Opening a separate court proceeding in the target state (often called a miscellaneous, ancillary, or special proceeding) to obtain court approval from the target state to issue the subpoena.

Before taking any action in the target state, counsel should consult the target state's rules of civil procedure and the court's local rules to ensure compliance.

Deposition Questions: To Plaintiff in a Single Plaintiff Discrimination Case

Model questions for an employer's counsel to use when deposing the plaintiff in a single plaintiff discrimination case under Title VII of the Civil Rights Act of 1964 (Title VII), the Americans with Disabilities Act (ADA), the Age Discrimination in Employment Act (ADEA), or the Genetic Information Nondiscrimination Act (GINA). This Standard Document applies to cases involving private employers. It is based on federal law. This Standard Document has integrated notes with important explanations and drafting tips.

DEPOSITION QUESTIONS: PLAINTIFF IN A SINGLE PLAINTIFF DISCRIMINATION CASE

Plaintiff's Education and Work Experience

- [Please describe your education./Did you attend high school? If yes:
  - which high school?
  - did you graduate?
  - when did you graduate?
  - what did you do after graduation?]
- Did you attend [college/vocational school/an apprenticeship program]? If yes:
  - which [school/program]?
  - what was your [major/area of focus]?
  - did you graduate?
  - when did you [graduate/complete the program]?
  - what [degree/certificate] did you earn?
  - what did you do next?
- Did you attend graduate or professional school? If yes:
  - which school?
  - what was your area of focus?
  - did you graduate?
  - when did you graduate?
  - what degree did you earn?
  - what did you do after graduation?
- Please explain any gaps in your education.
- Do you have any professional [certificates/licenses/credentials]? If yes:
  - which [certificates/licenses/credentials]?
  - when did you obtain each [certificate/license/credential]?
- Please describe your work experience.
- For [PAST EMPLOYER], when did you begin working for that employer?
- For [PAST EMPLOYER], when did your employment for that employer end?
- For [PAST EMPLOYER], what positions or job titles did you hold?
- For [PAST JOB], what were your job duties and responsibilities?

- For [PAST JOB], who were your supervisors?
- For [PAST JOB], what was your compensation, including base pay and any bonuses or other compensation?
- For [PAST JOB], were you ever disciplined, counseled, or suspended at work? If yes, please describe.
- For [PAST JOB], why did you leave that position?
- Are you eligible for rehire with [PAST EMPLOYER]? If not, why?
- For [PAST JOB], where did you work next?
- Were you ever fired, demoted, or asked to resign from a job? If yes, please explain.
- Please explain any gaps in your work experience.
- Do you have any documents related to your [PAST JOB]? Have they been produced? If not, why?

Application and Employment with the Defendant Employer

- When did you first apply for a job with [EMPLOYER NAME]?
- What position did you apply for?
- How did you learn about the position?
- How did you apply?
- Please describe the application and interview process.
- With whom did you interview?
- When were your interviews?
- Where did your interviews take place?
- Were you hired?
- [Why were you/What is your understanding of why you were] [not] hired? What is the basis for your understanding?
- [Who/What is your understanding of who] made the decision to [not] hire you? What is the basis for your understanding?
- How did you learn you were [not] hired?
- When were you [informed that you were not] hired?
- For which position were you hired?
- What was your job title?
- When did you start in that position?
- To whom did you report?
- Please describe your job responsibilities and duties.
- Did your job responsibilities and duties ever change? If yes:
  - when?
  - why did they change?
  - how did they change?
- What was your [initial] compensation, including both base rate of pay and any bonuses or other compensation?
- Were you eligible for a bonus?
- If yes, did you receive any bonus?
- Were you eligible for benefits?
- If yes, what benefits?
- Did your compensation ever [change/increase/decrease]? If yes:
  - when?
  - by how much?
  - why?
- How long did you remain in that position?
- Did you change positions at any point? If yes:
  - when?
  - why did you change positions?
  - did you voluntarily change positions?
  - did you ask to change your position?
  - were you [promoted/demoted/transferred]?
  - who made the decision to change your position?
  - to which position did you change?

- what was your new job title?
- when did you start in that position?
- to whom did you report?
- please describe your job responsibilities and duties.
- did your compensation change with the new position? If so, please explain how it changed.
- how long did you stay in that position?

- Were you ever disciplined by [EMPLOYER NAME/SPECIFIC SUPERVISOR, IF RELEVANT]? If yes:
  - when?
  - for what conduct?
  - who made the decision to discipline you?
  - what is the basis for your understanding?
- Were you ever suspended from work with [EMPLOYER NAME]? If yes?
  - was it with or without pay?
  - what [event/conduct] led to your suspension?
- Were you ever placed on a [performance improvement plan/PIP]? If yes:
  - what were the terms of the plan?
  - what did you need to do to get off the plan?
  - did you accomplish the goals of the plan?
- Did you ever receive a performance evaluation? If yes:
  - when?
  - was it in writing?
  - who evaluated your performance?
  - who delivered your review?
  - on what basis were you evaluated?
  - did you agree with your review?
  - if no, why?
  - if no, did you tell someone you disagreed? who?
  - did you ever prepare a self evaluation?
- Are you currently employed by [EMPLOYER NAME]? If yes, in what position? If no, when did your employment with [EMPLOYER NAME] end?

Factual Basis for Specific Allegations and Defenses

- Please [explain the allegation in your complaint that [ALLEGATION]/describe [CIRCUMSTANCES RELATING TO THE ALLEGATION]/describe the events and circumstances that you claim were discriminatory].
- Please explain what happened.
- Where did it take place?
- When did it take place?
- Who was involved? Anyone else?
- What was [NAME/DESCRIPTION OF PERSON]'s role?
- What did [NAME/DESCRIPTION OF PERSON] say or do? Anything else?
- What was your role?
- What did you say or do?
- Did you object?
- Was anyone else present? If yes, who? What was [his/her] role?
- Did anyone else see [EVENT]? If yes:
  - who?
  - anyone else?
- What [did [NAME/DESCRIPTION OF PERSON] see/is your understanding of what [NAME/DESCRIPTION OF PERSON] saw]? What is the basis for your understanding?
- Did anyone else hear [EVENT]? If yes, who? Anyone else?
- What [did [NAME/DESCRIPTION OF PERSON] hear/is your understanding of what [NAME/DESCRIPTION OF PERSON] heard]? What is the basis for your understanding?

- What happened next?
- What about [EVENT] do you believe was discriminatory? What is the basis for your belief?
- Please explain the basis for your allegation that [ALLEGED ADVERSE ACTION] was based on your [PROTECTED CLASS STATUS].
- Did anyone make statements that you believe suggest discrimination? If yes:
  - who?
  - when?
  - where?
  - what was said?
  - why do you believe that statement suggests discrimination?
- Did anyone overhear those statements? If yes:
  - who?
  - anyone else?
- Are there any documents that you believe suggest discrimination? If yes:
  - which documents?
  - did you produce them? If not, why not?
  - why do you believe they suggest discrimination?
- Were there any other events or circumstances that you claim were discriminatory?
- Please confirm you have listed all instances of discrimination against you.
- Do you believe that you were treated less favorably than other employees? If yes:
  - please identify all employees that you believe were treated more favorably than you.
  - please describe how [OTHER EMPLOYEE] was treated more favorably than you.
  - what is your understanding as to why [OTHER EMPLOYEE] was treated more favorably than you?
  - who [is/was] [OTHER EMPLOYEE]'s supervisor?
  - what [is/was] [OTHER EMPLOYEE]'s compensation?
  - what [is/was] [OTHER EMPLOYEE]'s position or title?
  - what [are/were] [OTHER EMLOYEE]'s job duties and responsibilities?
  - what is [OTHER EMPLOYEE]'s educational background?
  - what is [OTHER EMPLOYEE]'s work experience with [EMPLOYER NAME]?
  - what is [OTHER EMPLOYEE]'s work experience prior to working for [EMPLOYER NAME]?
- [Are you aware of [EMPLOYER NAME]'s policy against [discrimination/harassment]?
  - did you receive a copy of it [when you were hired/each year]?
  - how did you receive it (for example, hard copy, an electronic notice, or through some other mechanism)?
  - did you sign an acknowledgment of receipt? did you click on something acknowledging receipt?]
- Did you report the [ALLEGED DISCRIMINATION] to anyone affiliated with [EMPLOYER NAME][in accordance with [EMPLOYER NAME]'s anti-[discrimination/harassment] policy]? If no, why not? If yes:
  - to whom did you report the [ALLEGED DISCRIMINATION]?
  - when did you report the [ALLEGED DISCRIMINATION]?
  - what was the substance of your report?
  - did you make your report orally or in writing? If in writing, did you produce a copy of your written report? If not, why not?
  - did anyone respond to your report? If yes, how did [NAME/EMPLOYER NAME] respond to your report?
  - did you believe that the response was adequate?
  - if you believe that the response was not adequate, why was it inadequate?
  - if you believe that the response was not adequate, did you follow up? If yes, what did you do to follow up? What happened?

Plaintiff's Membership in a Protected Class

- Your complaint alleges that you were discriminated against on the basis of your [PROTECTED CLASS CHARACTERISTIC], correct?
- Do you claim that you were discriminated against on any other basis?
- Did [DECISION MAKER] know that you are [A MEMBER OF THAT PROTECTED CLASS]? What is the basis for

your understanding?

- Did you meet [DECISION MAKER] in person?
- Did you speak with [DECISION MAKER]? By what means, meaning telephone, email, or other means?
- Did you tell [DECISION MAKER] that you are [A MEMBER OF THAT PROTECTED CLASS]?

Monetary Damages

- In your complaint, you seek damages of $[AMOUNT]. What is your basis for seeking those damages?
- In response to Interrogatory No. [NUMBER], you provided a calculation of your damages. Please explain that calculation to me.
- Have you engaged any expert witnesses to testify about your damages? If yes, who?

Damages for Emotional, Mental, or Physical Injuries

- Please describe any injuries you sustained as a result of the alleged unlawful discrimination.
- Did you suffer any emotional injuries as a result of the alleged unlawful discrimination?
- Did you suffer any mental injuries as a result of the alleged unlawful discrimination?
- Did you suffer any physical injuries as a result of the alleged unlawful discrimination?
- For each injury, what were your symptoms?
- For each injury, did you seek any medical treatment or other healthcare for the injury? If no, why not? If yes:
  - when?
  - who was your treating physician or healthcare provider?
  - what was your diagnosis?
  - what treatment did you receive?
- Were you ever hospitalized for any of these injuries? If yes:
  - for which injuries were you hospitalized?
  - when were you hospitalized?
  - to which hospital were you admitted?
  - who was your treating physician?
  - what treatment did you receive?
- Did you take any medication for any of these injuries? If yes:
  - which medications?
  - for each medication, who [is/was] the prescribing physician?
  - for each medication, how long did you take it?
  - for each medication, are you still taking it?
  - for each medication, what dose [do/did] you take?
  - for each medication, please describe why you [take/took] it and what symptoms it treated.
- How are you now? Have the [symptoms/injuries] resolved?
- Have the [symptoms/injuries] prevented you from [working/seeking work]?
- Have you engaged an expert to testify about any of these injuries? If yes, who?
- Before [DATE], did you seek treatment from any mental healthcare professionals? If yes:
  - when?
  - for what purpose?
  - which mental healthcare professionals did you consult?
  - what was your diagnosis?
  - please describe your treatment.
  - were you prescribed any medications as part of your treatment? If yes, please explain.
- Before [DATE], did you experience any [symptoms/injuries]? If yes:
  - please describe the [symptoms/injuries].
  - when did you experience these [symptoms/injuries]?
  - did you seek treatment for these [symptoms/injuries]? If so, what treatment did you receive? When did you receive treatment? Who was your treating physician or healthcare professional?
  - had these [symptoms/injuries] resolved before [DATE]?
- Do you use any social media cites (such as Facebook, LinkedIn, Twitter, Instagram, or Snapchat)? If yes, under what [name/user name/handle]?

Back and Front Pay Calculations

- [For your [back/front] pay claim, for what period of time did you calculate [back/front] pay?
- What salary and other benefits did you include in your [back/front] pay calculation?
- What other income, from any source, did you receive during this time period?
- Did you make any deductions from your [back/front] pay calculation for the other income received?]

Mitigation of Damages

- [For your [back/front] pay claim, for what period of time did you calculate [back/front] pay?
- What salary and other benefits did you include in your [back/front] pay calculation?
- What other income, from any source, did you receive during this time period?
- Did you make any deductions from your [back/front] pay calculation for the other income received?]
- What jobs have you held following the termination of your employment with [EMPLOYER NAME]?
- For [JOB], what was your compensation?
  - Did you receive any bonuses? Commissions? Other benefits?
- For [JOB], when did you start working there?
- For [JOB], are you still working there? If no:
  - when did you stop working there?
  - why did you leave that position?
  - were you fired or demoted? If yes, why?
- Please describe the efforts you have taken to find a job.
- How much time have you spent each [day/week/month] [since the termination of your employment with [EMPLOYER NAME]?
- Have you taken any vacations since the termination of your employment? If so, for how long? Did you engage in any job search activities while on vacation?
- Were you unavailable to work (due to illness or injury unrelated to your employment with [EMPLOYER NAME]) since the termination of your employment?
- Are you attending school or taking any classes? If so, full-time or part-time? Is this a degree program?
- Have you submitted your resume or job applications for any positions? If not, why not? If yes:
  - what jobs did you apply for?
  - when did you submit your application(s)?
  - what happened?
  - did you interview for any jobs?
  - were you offered any jobs? If yes, please explain.
- Have you used any [recruiters/staffing agencies/outplacement firms] to help you find a job? If no, why not? If yes:
  - [who/which agency(ies)]?
  - when?
  - what happened?
- Please describe any education or training you have received since the termination of your employment with [EMPLOYER NAME].
- Have you received any other income since the termination of your employment with [EMPLOYER NAME]?
- Have you been self-employed for any period of time since the termination of your employment with [EMPLOYER NAME]? If yes, how much money did you earn?
- Have you received any long-term or short-term disability insurance benefits? If yes, how much?
- Have you received any social security benefits, including social security disability insurance benefits? If yes, how much?
- Have you received any workers' compensation benefits? If yes:
  - how much did you receive?
  - for what period of time?
  - did you testify in any hearing or proceeding regarding these workers' compensation benefits? If so, when? Where?
- Have you received any unemployment insurance benefits? If so:
  - how much did you receive?
  - for what period of time?

- did you testify in any hearing or proceeding regarding these unemployment insurance benefits? If so, when? Where?
- [Have you received an offer of reinstatement by [EMPLOYER NAME]? If yes:
  - did you accept it? If so, when? If not, why not?
  - what were the terms of the offer?
  - were the terms substantially similar to your former employment? If not, in what way[s] did they differ?]

Witnesses or Evidence Corroborating Discrimination

- [Other than your lawyer,] [D/d]id you discuss [ALLEGED DISCRIMINATION] with anyone?
- Who did you discuss [ALLEGED DISCRIMINATION] with?
- When did the discussion take place?
- Where were you during the discussion?
- Was the discussion [in person/on the telephone/by email/through social media]?
- For each discussion, what was the substance of the discussion? What did you say? What did the other person say? How did the discussion end?
- [Other than your lawyer,] [D/d]id you discuss [ALLEGED DISCRIMINATION] with anyone else?
- Do you keep a journal or diary? If yes:
  - did you write anything about the [ALLEGED DISCRIMINATION] in your [journal/diary]?
  - did you produce a copy of your [journal/diary] in response to [EMPLOYER NAME]'s discovery requests?
  - do you still have your [journal/diary]? If not, why not?
- [Other than your lawyer,] [D/d]id you have any written communication, such as email, with anyone about the [ALLEGED DISCRIMINATION]?
- Please describe the written communications.
- Who did you [email/communicate] with?
- When did you [email/communicate] with [NAME]?
- What was the substance of your communication? What did you write? What did the other person write? How did the communication end?
- Do you have a copy of these writings?
- Did you post anything relating to the [ALLEGED DISCRIMINATION] on social media, such as Facebook, Twitter, or LinkedIn? If yes:
  - what did you post?
  - when did you post it?
  - did anyone respond to your post(s)?
  - do you have copies of your post(s)?

First Steps for Identifying and Preserving Electronic Information Checklist

A Checklist addressing the key issues a party should consider when identifying and preserving potentially responsive documents and electronically stored information in litigation.

This Checklist addresses the key issues a party should consider when identifying and preserving potentially responsive documents and **electronically stored information** (ESI) in litigation.

Preservation Obligation

- Once an organization reasonably anticipates litigation, it has a duty to preserve documents and ESI that it reasonably expects are relevant to the anticipated litigation. An organization may reasonably anticipate litigation prior to the actual filing of a complaint. For example, an organization may reasonably anticipate litigation once it receives a cease and desist letter, once a grievance is filed, or even after an informal discussion in which another entity threatens litigation. Determining whether any particular event should cause an organization to reasonably anticipate litigation is a case-specific analysis.
- In general, the preservation obligation requires that a party take reasonable steps to prevent the modification or deletion of information in its possession, custody, or control that it knows, or should know, is reasonably likely to be relevant and proportional to a pending (or reasonably anticipated) litigation or investigation. A party is not required to take heroic steps to preserve all documents or ESI.

Understand the Scope of Litigation and Communicate with Representatives in the Organization

- Review the information that triggered the duty to preserve, such as the complaint, summons, **subpoena**, formal notice, letter threatening suit, employee report, or other available documentation.
- Communicate the nature of the litigation and obligations to representatives from:
  - legal;
  - information technology (IT);
  - risk management;
  - records management;
  - human resources;
  - other impacted departments or business units;
  - affiliated entities or third parties within the organization's control; and
  - insurance carriers, as appropriate.

Determine the Need for Emergency Preservation

- Identify any pertinent data sources or relevant information that are at risk due to imminent destruction, such as:
  - dynamic databases;
  - former employee data;
  - email or text messages with janitor systems or auto-delete functions; and
  - material information in unallocated space (for example, deleted, residual, or fragmentary data).
- Take steps reasonably quickly to protect potentially relevant information.

Identify Sources of Potentially Relevant ESI

- Identify key employees and third parties most likely to possess potentially relevant data.
- Interview IT representatives and other employees to determine what potentially relevant information is stored on:
  - network email and other accounts;
  - laptop and desktop computers;
  - databases;
  - Sharepoint or other collaborative workspaces;
  - applicable websites; and
  - outsourced locations.

  For more information about record manager interviews, see Data Collection: Questions to Ask Records Department Personnel Checklist.
- Determine whether potentially relevant information may be within an individual employee's control, for example, on:
  - smartphones;
  - personal digital assistants;
  - tablets;
  - USB or flash drives;
  - personal email accounts;
  - personal laptop or desktop computers;
  - personal cell phones; or
  - **social media** sites, such as Facebook and Twitter.

  For more information about custodian interviews, see Standard Document, Data Collection: Document Custodian Interview Questions.

Take Initial Steps to Preserve ESI

Before issuing a litigation hold notice:

- Identify employees with a potential incentive to delete data (for example, a supervisor accused of harassment or an employee accused of theft).
- Take covert steps to collect and secure information from employees with a potential incentive to delete data.

Develop and Issue the Litigation Hold Notice

Draft the Litigation Hold Notice

- Outline the types of materials, including paper documents and ESI, to be retained and identify the employees who may possess those materials.
- Identify the relevant time frame to which the preservation obligation applies.
- Remember that the notice itself may eventually be disclosed to opposing parties or the court.
- Consider third parties (for example, corporate affiliates) who may possess documents and ESI under the organization's control and determine whether they should receive the notice or a separate letter requesting preservation. Consider using a separate notice for third parties that do not have a privileged relationship with the organization.

Issue the Litigation Hold Notice to Employees and Third Parties

- Issue a written **litigation hold** notice (also known as a document preservation notice or a legal hold) to employees who may possess potentially relevant material (see Standard Document, Litigation Hold Notice).
- Remember to notify the records manager/coordinators and IT representatives about the hold notice.

Confirm Receipt and Understanding of the Litigation Hold Notice

- When the litigation hold notice is issued, identify a specific person who will track the execution, collection, and retention of the signed acknowledgements described below.
- Have each recipient of the litigation hold notice sign a document acknowledging that they:
  - received the litigation hold notice;
  - understand it; and
  - intend to comply with it.
- Collect and retain signed acknowledgements from each recipient of the litigation hold notice.

Update and Issue Periodic Reminders of the Litigation Hold Notice

- Identify a specific person who will be responsible for the litigation hold notice going forward. This person will:
  - make necessary revisions to the scope of the litigation hold notice and inform all recipients of the same;

- draft and circulate regular, periodic reminders of the litigation hold notice while it remains in effect; and
- document all revisions and reminders to maximize the defensibility of the preservation process.

Preserve Various Data Sources

- When selecting a preservation protocol, a party should be mindful of the impact that various preservation methods can have on **metadata**. Unless a party has confirmed that all opposing parties will not seek metadata, the party should take reasonable steps to preserve it.
- Consider whether litigation risks justify creating a forensically sound logical copy or mirror image (for example, a bit-by-bit image) of network email accounts, local hard drives, network directories, or other employee data sources that are likely to have responsive documents. If copies are going to be made:
  - determine an appropriate timetable for copying data; and
  - segregate and preserve any copies made in a secure repository.
- If employees' network accounts and directories are not imaged, develop an alternative preservation plan for network data sources.
- If key players' hard drives are not imaged, develop an alternative preservation plan.
- Balance data privacy concerns against the need to preserve potentially relevant information quickly.
- Determine whether potentially relevant data may exist in databases, such as a document management system or Sharepoint, and whether that data may be vulnerable to modification or deletion.
- Develop a plan to preserve potentially relevant data that may be subject to alteration or deletion. For example, sensitive files may be copied, sequestered, or removed from local or network drives, before a litigation hold is issued to employees.

Develop a Plan for Dealing with ESI that is Not Reasonably Accessible

- The touchstones for preservation, and all of discovery, are relevance and reasonableness.
- Determine whether the organization's archives and backup tapes are reasonably accessible. Generally, a party is only required to preserve information that is reasonably accessible at the time the duty to preserve is triggered, unless the information is unique and material (that is, under the totality of the circumstances, the value of the information is greater than the cost to preserve it).
- Investigate the organization's archival and backup practices and the existence of potentially relevant legacy data.
- Consider whether to continue normal recycling of backup tapes.
- Consider withdrawing specific backup tapes from the normal rotation cycle and preserving them:
  - for the duration of the litigation; or
  - until the parties can reach an agreement about whether the backup tapes need to be preserved.

Consider Data of Transferring and Departing Employees

- Develop a procedure for preserving the data of transferring and departing employees who may possess potentially relevant information.
- Collect and secure all potentially relevant information from transferring, departing, and departed employees' hard drives and other devices that may become unavailable.

Document Preservation Activity

- Document the steps that the organization takes to preserve relevant documents and ESI and the reason for those steps.
- Document preservation steps considered but not completed, as well as the reasons for not taking those steps.
- Contemporaneously documenting why certain decisions were made may:
  - help demonstrate that reasonable efforts were taken in good faith; and
  - increase the defensibility of the process.

For a sample log for tracking compliance with a litigation hold notice, see Standard Document, Data Collection: Tracking a Litigation Hold Template.

Consider Negotiating with Opposing Parties

- Consider negotiating a reasonable document preservation plan with opposing parties as early as possible. If an organization understands what opposing parties will seek in discovery, it can more defensibly tailor its preservation efforts.
- The **meet and confer** process can be an effective tool to limit the scope of discovery and drive desired results.
- Discuss the scope of discovery (including the need for metadata) and what is proportional to the needs of the case, considering:
  - the importance of the issues at stake;
  - the amount in controversy;
  - the parties' relative access to relevant information;
  - the parties' resources;
  - the importance of the discovery in resolving the issues; and
  - whether the burden or expense of the proposed discovery outweighs its likely benefit.
- If the parties cannot reach an agreement on the scope of preservation, consider making a motion for a **protective order**.

For more information about the meet and confer process, see Rule 26(f) Conference Checklist.

Data Collection: Locating and Collecting Relevant Data

Model questions for counsel when interviewing IT personnel or any person with knowledge of how data is managed, organized, and stored within the company to effectively identify and gather information about possible locations of information relevant to the dispute. This Standard Document has integrated notes with important explanations and drafting tips.

[CASE TITLE]: Document Collection

Interviewee's Name:

Attorney's Name:

Date:

Background and Litigation Hold

- What is your name?
- What is your job title?
- Please describe the responsibilities of your current position.
- How long have you been in your current position?
- Did you receive a litigation hold in connection with [CASE DESCRIPTION]?
- When and how did you receive it?
- Have you taken any action in response to the litigation hold? If yes:
  - what have you done?
  - did you stop any routine destruction of information?
  - when did you stop?
  - what information was stopped from routine destruction?
  - how did you identify what information to preserve?
- Have there been any data purges after [DATE OF LITIGATION HOLD]? If yes:
  - how many?
  - when [was it/were they]?
  - what information was deleted?
  - is that data still accessible? If yes, describe how that information can be obtained and where it is located.
- With whom have you spoken about the dispute or litigation hold and what did you discuss with:
  - employees in the IT department?
  - employees in the records department?
  - document custodians?
  - vendors and third parties outside of the company?
  - anyone else?

- Have you been involved with other litigation holds during your employment at [COMPANY]? If yes:
  - for how many cases?
  - how much data was involved?
  - what was your involvement in the litigation hold[s]?

Document Retention Policy

- What document retention policies does [COMPANY] have?
- When [was it/were they] last updated?
- How many versions have there been?
- Under the policy, for how long does the company keep:
  - emails?
  - instant messages?
  - other communications?
  - [OTHER RELEVANT INFORMATION]?
- Are there records or logs that identify information that is destroyed? If yes, how long are the records or logs retained?
- Are you aware of any information that was destroyed that may be relevant to this litigation?
- Does the company purge data regularly? If yes:
  - how often?
  - is the company current with its document retention policy?
  - is data deletion automated?
  - who is responsible for enforcing the company's document retention policy?
- [If the company does not regularly purge data, explain in what way the company is not consistent with its document retention policy?]

File Servers, Shared Networks, and Backup Systems

- How many file servers does the company have?
- Where is each server located?
- What kind of information is on each server?
- Do all users have access to a shared network? If not:
  - how do users' access differ?
  - are any shared network folders available to all users?
  - which shared networks may be accessed by users in [RELEVANT BUSINESS UNITS]?
- Do users have a personal server drive?
- How is each server secured?
- What does the company do with former employees' files?
- Who is responsible for the maintenance and operation of the network?
- What kind of backup systems does the company use?
  - tape or digital?
  - local or remote?
- If the company uses a tape backup system:
  - how many tapes are used?
  - are they rotated?
  - where are the tapes located?

- How much information is backed-up typically?
- How much data is currently backed-up?
- How are the backup systems organized or catalogued?

Email

- What email system does the company use?
- What software is used for email and which version is used?
- What hardware is used for email?
- Where is the email system managed?
- Have there been any other email systems used? If yes:
  - what email system was it?
  - when was this email system last used?
- Where are the email servers located?
  - how many email servers does the company have?
  - if there is more than one server, how are users assigned to a server?
- How many users are on the email system currently?
- Who is responsible for maintenance and operation of the email system?
- Can users access email remotely? If yes:
  - with what system (Citrix, Webmail, or something else)?
  - can users store data on their personal computer when accessing email remotely?
- Can emails be stored locally or on removable media?
- Where are emails saved by default?
- Are deleted messages retained on the server?
- Is there a size limit to each user's inbox?
- Is there an archiving system? How does it work?
- What are the server retention or archive settings?
- Does the company have an email backup system? If yes:
  - what type is it?
  - tape or digital?
  - local or remote?
  - automated?
- If the company uses a tape backup system, how many tapes are used? Are they rotated?
- What is the size of the backup?
- How are the backup systems organized or catalogued?
- How often does the company perform back-ups?
- Are emails purged regularly? If yes:
  - how often does the company purge emails?
  - what is the purging policy?
  - how long do messages stay in the [inbox/sent mail folder/delete folder/draft folder]?
- Are former employees' accounts maintained? If yes:
  - how are they maintained?
  - where are they maintained?
  - for how long are they maintained?

- how accessible is the information?

- Can employees send secure messages?
- Does the company have encryption software? If yes:
  - what messages are encrypted?
  - how can employees send encrypted messages to third parties?
  - how can employees access encrypted messages from third parties?
  - who has access to encryption passwords?

Company-Issued Hardware and Software

- What type(s) of computers are company employees issued (for example, desktops, laptops, tablets, or something else)?
- What are the make and models of the computers?
- How often does the company upgrade computers?
- When computers are upgraded, how is data transferred to the new computers?
- Describe the process for re-imaging a desktop or laptop.
- Are users able to save files locally to their issued computers?
- What is the policy on users saving files to their work-issued and personal computers?
- Are any computers shared?
- What happens to the computers used by former employees?
  - what happens to the data stored on the computers?
  - are the computers ever re-issued to other employees?
  - may employees keep their computers after leaving the company?

- How are usernames assigned?
- How often must users change their passwords?
- Does the company use any collaborative systems (for example, SharePoint)? If yes:
  - where is that data stored?
  - is it password protected?
  - how often is the password changed?
  - is there a log of individuals who use or access the system?

- What software does the company use that may contain relevant information?
- What databases does the company use that may contain relevant information?
- Does the company keep logs? If yes, of what?
- Does the company use any proprietary software that may be relevant? If yes:
  - what is it?
  - what relevant information may be available using the software?
  - who maintains the software?
  - how long has the company used the software?
  - did the company use legacy proprietary software during the relevant time frame?

- Are employees permitted to download software on their work-issued computers?
- Are employees permitted to download work-related materials or software on their personal computers?

Handheld Devices

- Does [COMPANY] have a Bring Your Own Device to Work (BYOD) policy?
- Does [COMPANY] issue handheld devices such as cell phones or tablets? If yes:

- to whom?
- what type and model?
- how often is a new model issued to employees?
- what happens to the replaced device?
- what happens to the data on the replaced device?
- are company-issued cell phones or tablets ever re-issued to other employees?
- does the company permit employees to keep the devices after leaving the company?

- Does [COMPANY] support cell phones or tablets? If yes:
  - for whom?
  - any specific types and models?
  - what support is provided?

- Can users access their personal email accounts on a handheld device that is issued or supported by the IT department? If yes, how?
- Are [emails/instant messages/voicemails/data/calendars] that are received or maintained on a handheld device also stored on a company server?
- Is email that is sent or received on a handheld device synced to a company server?
- Is there any data on the handheld device that would not be stored on a company server?
- What is the company's security policy on handheld devices?
- Describe the process when a handheld device is re-imaged.

Information on the Cloud

- What kind of information does [COMPANY] have on the cloud?
  - how is the information used by [COMPANY]?
  - can the data be searched?
  - is there a firewall to protect the information stored on the cloud?

- Who is responsible for maintaining and managing the company's information that is stored on the cloud?
- What cloud storage vendors does the company use?
  - do the vendors have their own servers or do they purchase them elsewhere?
  - are there written contracts with these vendors? If yes, may we receive a copy?
  - what is the vendor's backup policy?
  - has every vendor received a copy of the litigation hold?

- What kind of internet security does the company have?
- Does the company allow employees to use social media sites at work?

Instant Messaging

- Does the company have an internal instant messenger? If yes:
  - what type?
  - how is it used?
  - does the company have any instant messaging policies?

- Are instant messaging conversations preserved? If yes:
  - for how long are they preserved?
  - is the preservation automatic or must they be manually preserved by the user?

- Are there any modes of internal communication other than email and instant messaging? If yes, can the communications be preserved?
- May employees install and use external instant messengers?

Voicemail

- Does [COMPANY] have any voicemail storage policies?
- Is voicemail automatically stored? If yes, for how long?
- If voicemail is manually stored, how long may it be stored by a user?
- Are voicemails also received by the recipient by email?

Data Collection: Document Custodian Interview Questions

Model questions for counsel interviewing company employees about documents and other materials that may be in their possession and that are potentially relevant to a lawsuit, dispute, investigation, or audit. This Standard Document has integrated notes with important explanations and drafting tips.

[CASE TITLE]: Document Collection

Custodian's Name:

Attorney's Name:

Date:

Background

- What is your name?
- What is your education?
- What is your job title?
- Please describe the responsibilities of your current position.
- When did you start working for [COMPANY]?
- When did you start your current position?
- Did you have any previous positions with the company? If yes:
  - what position[s] did you have?
  - when did you have [that/those] role[s]?
- Do you have any secretaries or assistants working directly for you? If yes:
  - who?
  - how long has [NAME] been your [secretary/assistant]?
  - during what time period?
  - does [he/she] have access to your calendar?
  - does [he/she] have access to your files?
  - [have you had any other secretaries or assistants who worked directly for you between the dates [RELEVANT TIME PERIOD]?]
- Do you use a desktop or laptop at work? If a laptop:
  - do you bring it home to do work on it?
  - [how often do you bring it home?]
- Do you work remotely? If yes:
  - from what location?
  - how often?
  - what kind of work do you do at [home/[LOCATION]]?
  - do you use a work-issued computer, tablet, or other device when you work remotely?

- do you use a personal computer, tablet, or other device when you work remotely?
- what computers or other devices do you have at [home/[LOCATION]] that you have used for work purposes?
- how long have you had each device?
- does your personal computer contain any work-related documents?

- Have you had any other computers or other devices that you used at [home/[LOCATION]] for work during [RELEVANT TIME PERIOD]? If yes:
  - what devices did you have?
  - do you still have [it/them]?
  - what did you do with the device[s] that you no longer use?
  - [is/are] the device[s] still accessible?
  - [is/are] the device[s] in your possession?
  - where [is it/are they]?
  - did you wipe data off the device[s] before you discarded [it/them]?
  - [does that/[do/did] any of those] device[s] contain relevant information?
  - [can that information be retrieved?]

- Have you seen the litigation hold? If yes:
  - do you [still] have a copy of it?
  - when did you receive it?
  - from whom did you receive it?
  - how did you receive it (for example, by email or hard copy distribution)?

- Are you familiar with the facts of the dispute underlying the litigation hold? If yes:
  - what documents do you think are relevant to this dispute?
  - what types of documents did you create or receive relating to this dispute?

- What steps have you taken in response to the litigation hold so far?
  - have you preserved any data?
  - what steps have you taken to preserve data?
  - when did you start looking for relevant documents?
  - when did you start preserving relevant documents?

- Have you checked all locations at [home/[LOCATION]] (for example, home office, desks, paper files, home computers, and mobile devices) for potentially relevant information?

Email

- What is your email address at work?
- Have you had any other work email addresses?
- Have you changed your email configuration from [COMPANY]'s default? If yes:
  - how have you changed it?

- Does your email inbox have a space limit? If yes:
  - what do you do when you reach the inbox space limit?

- Do you save emails? If yes:
  - where do you save them?

- do you have folders set up? If yes, do you have any folders set up that contain emails relating to this dispute?
- do you save them to your computer locally or to the shared network?
- have you ever saved emails to a USB drive, CD, or other storage device? If yes, what happened to that media?
- do you save emails by forwarding them to a non-work email account?

- Do you actively delete emails? If yes:
  - what emails do you delete?
  - how do you delete them?
  - do you delete "deleted emails"?
  - [how frequently do you do this?]

- Are emails automatically deleted? If yes:
  - how often are they deleted?

- Do you check your work email on a portable device (for example, a cell phone or tablet)? If yes:
  - what kind of portable device do you use?
  - is your [DEVICE] company-issued?
  - how do you access work email through your [DEVICE]?
  - is your work email routed to your [DEVICE]?
  - is your personal email routed to your [DEVICE]?

- Do you access work email at home? If yes:
  - on what type of computer or portable device do you access it (for example, computer, tablet, or cell phone)?
  - how do you access it (for example, Citrix, VPN, Webmail, or Outlook Express)?

- Do you forward work-related emails to your personal email account? If yes:
  - how many personal email accounts do you have?
  - how many personal email accounts have you used for work?
  - what [is/are] your personal email address[es] to which you have sent work-related emails?

- Do you have a personal computer at home? If yes:
  - who is your internet provider?
  - have you downloaded or saved any emails or other work-related material to your home computer?
  - do you open work-related email attachments on your home computer?
  - do you ever print your work-related emails at home?
  - do you have any emails related to this dispute at home?

Handheld Devices (Cell Phones and Tablets)

- Do you have a cell phone or tablet that was issued by [COMPANY]? If yes:
  - what is the make and model?
  - was your [cell phone/tablet] set up by [COMPANY]?
  - do you receive text messages on your [cell phone/tablet]?
  - do you use your [cell phone/tablet] for other types of chats?
  - have you sent or received any work-related text messages [or chats] from your [cell phone/tablet]?
  - have you accessed work email from your [cell phone/tablet]?

- do you receive work-related emails directly on your [cell phone/tablet]?
- do you have any work-related voicemails saved on your [cell phone/tablet]?
- have you used a calendar on your [cell phone/tablet] for work appointments or other work-related information?
- have you used any utilities on your [cell phone/tablet] for work, such as voice memos, reminders, or notes?
- do you have any photos or videos saved on your [cell phone/tablet] that relate to work?
- is there any other work-related data that may be on your [cell phone/tablet]?

- Do you have a personal cell phone or tablet? If yes:
  - what is the make and model?
  - was your [cell phone/tablet] approved by [COMPANY]?
  - was your [cell phone/tablet] set up by [COMPANY]?
  - do you receive text messages on your [cell phone/tablet]?
  - do you use your [cell phone/tablet] for other types of chats?
  - have you sent or received any work-related text messages [or chats] from your [cell phone/tablet]?
  - have you accessed work email from your [cell phone/tablet]?
  - do you receive work-related emails directly on your [cell phone/tablet]?
  - do you have any work-related voicemails saved on your [cell phone/tablet]?
  - have you used a calendar on your [cell phone/tablet] for work appointments or other work-related information?
  - have you used any utilities on your [cell phone/tablet] for work, such as voice memos, reminders, or notes?
  - do you have any photos or videos saved on your [cell phone/tablet] that relate to work?
  - is there any other work-related data that may be on your [cell phone/tablet]?

Calendars, Diaries, and To-Do Lists

- Do you use a calendar for work? If yes:
  - is it electronic (for example, Microsoft Outlook or on a handheld device), hard copy, or both?
  - do you have any calendar entries relating to this dispute?
  - [do you make handwritten notes on your hard copy calendars?]
  - [do you save your hard copy calendars?]
  - [how do you dispose of them?]
  - [how often do you dispose of them?]
  - [do you delete entries to your electronic calendar after an event occurs?]

- Do you use diaries to make notes? If yes:
  - are they electronic, hard copy, or both?
  - did you make any notes in your diaries relating to this dispute?
  - [do you save your hard copy diaries?]
  - [how do you dispose of them?]
  - [how often do you dispose of them?]

- Do you make to-do lists? If yes:
  - where do you write them?
  - do you use post-its?
  - what do you do with them after you complete the tasks?

- do you save them?

Instant Messenger

- Do you use an internal instant messenger at work? If yes:
  - with whom have you exchanged messages?
  - for what purpose?
- Do you use an external instant messenger (for example, Google Chat) at work? If yes:
  - with whom have you exchanged messages?
  - for what purpose?
- Do you use any other modes of internal instant communication?
- Do you recall using instant messaging in connection with the subject matter of this dispute? If yes:
  - have you saved any instant messaging conversations relating to this dispute?

Voicemail

- Do you save voicemails or do you normally delete voicemails after you listen to them?
- Do you ever transcribe (or have someone transcribe) voicemails before deleting them?
- Do you receive copies of your voicemails on email? If yes:
  - do you save them?
  - [where do you save them?]
- [Do you have any voicemails saved related to this dispute?]
- [Do you have any voicemail transcriptions of messages that relate to this dispute?]

Computer Files

- What types of documents do you generate or receive? For example:
  - Microsoft Word or other word processing documents;
  - Microsoft Excel or other spreadsheets;
  - Microsoft PowerPoint or other presentations;
  - PDFs; and
  - proprietary systems?
- On your work computer, where do you save files? Do you use:
  - a public network drive?
  - a personal shared drive?
  - the hard drive?
  - removable media, such as a USB or CD?
- Do you have any documents relevant to this dispute on your work computer? If yes:
  - what kind of files are they?
  - where and how are they stored?
- Do you transfer large files off of your work computer for use when you are not in the office? If yes:
  - do you use Dropbox, Google Drive, or another internet-based file-sharing service for work files?
  - have you used a USB to take files home?
  - did you ever transfer large files in connection with the subject matter of this dispute?

Social Media

- Do you use social media?
- Which forms of social media do you use (for example, Facebook, Twitter, LinkedIn, tumblr, or Instagram)?
- Is your [SOCIAL MEDIA] account public or private?
  - if private, who can view your account?
- How often do you use your [SOCIAL MEDIA] account?
- Have you ever discussed work-related issues on [SOCIAL MEDIA]? If yes:
  - in what regard?
  - who can see the activity?
  - did anyone respond to your activity? If yes, who and how?
- Do you interact with [COMPANY]'s social media accounts from your personal account?
- Have you posted anything related to this dispute on social media? If yes:
  - what did you post?
  - when did you post it?
  - [is/are] your post[s] public or private (to what extent is it private)?
  - did anyone respond to your post[s]?
  - do you have a copy of your post[s]?
- How do you access your [SOCIAL MEDIA] account?

Hard Copy Documents and Other Materials

- Do you take handwritten notes generally?
- When attending meetings, do you take notes? If yes:
  - what do you do with them?
  - do you have any notes from meetings related to this dispute?
- Do you use notebooks, legal pads, or other hard copy formats to write your notes? If yes:
  - do you save them?
  - where are they located?
  - do any of them have information related to this dispute?
- Where do you store your hard copy documents?
- Do you send any hard copy documents to [COMPANY]'s records department? If yes:
  - what do you send there?
- Do you have any hard copy work documents at home?
- Have you drafted any memoranda to file about this dispute? If yes:
  - where are these memoranda located?

Communications with Others

- Have you communicated with anyone regarding this dispute? If yes:
  - with whom?
  - what did you discuss?
  - did you communicate in writing? If so, describe.
- Do you know anyone else who would have relevant documents (including former employees)?

Document Requests: Common Problems with an RFP Response

This Practice Note addresses some common problems counsel face when receiving a response to a request for the production of documents (RFP) under ***Rule 34 of the Federal Rules of Civil Procedure*** *(FRCP). Specifically, this Note explains what counsel should do when they receive documents and electronically stored information (ESI) in a form different from that requested, an unmanageable production (also called a document dump), insufficient privilege designations, and inadvertently produced privileged documents.*

Contents

When receiving documents and **electronically stored information** (ESI) in response to a **request for the production of documents** (RFP), counsel may find problems with the producing party's response. This Note addresses common problems that counsel may face involving:

R

- The form and nature of the documents received.
- Information withheld based on asserted privileges.
- The inadvertent production of privileged material.

Counsel Do Not Receive the Documents as Expected

The producing party might not provide information in response to an RFP in the manner that counsel expects. This section covers when the producing party:

- Does not produce ESI in the form requested (see ESI Is Not Produced in the Form Requested).
- Does not produce ESI from all available sources (see ESI Is Not Produced from All Available Sources).
- Produces documents in another language (see Documents Are Produced in Another Language).
- Produces a voluminous and unmanageable document production (see The Document Production Is Too Voluminous and Unmanageable).
- Objects to the place for inspection of documents (see The Producing Party Objects to the Place for Inspection and Copying of Documents).
- Files a motion for a protective order (see The Producing Party Files a Motion for a Protective Order).

ESI Is Not Produced in the Form Requested

An RFP should specify the form of ESI that counsel would like to receive. If the producing party objects to the requested form, its RFP response should:

- State its objection to the requested form of ESI.
- Identify the form of ESI it intends to produce.

(FRCP 34(b)(2)(D).)

If the producing party does not object to the requested form of ESI but fails to produce ESI in that form, counsel should promptly notify the producing party of its obligation to produce ESI in the form requested and attempt to reach an agreement on the issue. If the parties cannot agree, counsel should promptly move the court to compel the production of documents in the requested format. Counsel should not delay making the motion because if the burden on the producing party to provide the requested form of ESI becomes too great, the court may deny the motion (see *Ford Motor Co. v. Edgewood Props., Inc.*, 257 F.R.D. 418, 424-26 (D.N.J. 2009) (denying motion to compel made after the entire document production was complete); see also *McSparran v. Commonwealth of Pennsylvania*, 2016 WL 687992, at *4 (M.D. Pa. Feb. 18, 2016) (finding that it would be unduly burdensome to require the plaintiff to redo her document production in response to the defendants' late request for metadata)).

Similarly, if the parties agreed to a particular form for production in their **meet and confer** under FRCP 26(f) (Rule 26(f) conference) but the producing party fails to produce ESI in the agreed-to form, counsel should promptly reach out to the producing party to resolve the issue and, if the parties cannot agree, move the court to compel production in the requested form. For more information on Rule 26(f) conferences, see Standard Document, Rule 26(f) Report and Discovery Plan and Rule 26(f) Conference Checklist.

If counsel fails to specify, or is vague about, the form of ESI requested, the producing party may produce ESI in the form in which the party usually maintains it (see *U.S. ex rel. Carter v. Bridgepoint Educ., Inc.*, 305 F.R.D. 225, 243 (S.D. Cal. 2015)).

ESI Is Not Produced from All Available Sources

When responding to an RFP, the producing party must state whether it is withholding any information on the basis of an asserted objection (FRCP 34(b)(2)(C)). When counsel receive documents, they should determine whether the producing party produced documents:

- As stated in the RFP response.
- From the sources of ESI identified in:
  - the producing party's initial disclosures under FRCP 26(a);
  - the Rule 26(f) discovery plan; and
  - the producing party's **document retention policy**.

For more information on initial disclosures, see Standard Document, Initial Disclosures and Practice Note, Initial Stages of Federal Litigation Overview: Initial Disclosures.

If counsel is concerned that the producing party is not disclosing that it withheld documents or that it is not producing ESI from all available sources, counsel should promptly confer with the producing party and may need to seek court intervention. Counsel must have a basis for claiming that the producing party is withholding ESI since a court will not compel the production of additional ESI based on mere speculation that it exists (see, for example, *Little Hocking Water Assn., Inc. v. E.I. Du Pont De Nemours & Co.*, 2013 WL 608154, at *10 (S.D. Ohio Feb. 19, 2013) (citing cases)).

The producing party must produce responsive ESI, even if they need to convert it into a reasonably usable form, so long as the burden of production does not outweigh its likely benefit (FRCP 26(b)(1), 34(a)(1)(A)). For example, if a producing party has responsive, accessible ESI that only can be viewed on proprietary software, it may produce the information in a reasonably usable format, such as **PDF** (see, for example, *Davenport v. Charter Commc'ns, LLC*, 2015 WL 1286372, at *3 (E.D. Mo. Mar. 20, 2015) (stating that courts regularly hold that PDFs are a reasonably usable format); *AKH Co. v. Universal Underwriters Ins. Co.*, 300 F.R.D. 684, 690 (D. Kan. 2014) (denying the plaintiff's request to compel the defendant to re-produce documents from certain software that is proprietary in nature in native form that it already produced in PDF form as requested by the plaintiff); *Adams v. AllianceOne, Inc.*, 2011 WL 2066617, at *7-8 (S.D. Cal. May 25, 2011)).

Documents Are Produced in Another Language

The producing party may have responsive documents in its possession or control that are in a language other than English. When a party produces a document that is in another language, the party:

- Does not need to translate the foreign language document (*Nature's Plus Nordic A/S v. Natural Organics, Inc.*, 274 F.R.D. 437, 442 (E.D.N.Y. 2011); *Tech-Sonic, Inc. v. Sonics & Mat., Inc.*, 2015 WL 4715329, at *9 (D. Conn. Aug. 7, 2015), as corrected (Aug. 24, 2015)).
- Must produce any existing translations or English summaries of the document (*Hui Qin Wong v. Jian Ping Yao*, 2013 WL 2304180, at *1 (E.D.N.Y. May 17, 2013); *Nature's Plus Nordic A/S*, 274 F.R.D. at 440).

The Document Production Is Too Voluminous and Unmanageable

A party must produce documents either:

- As they are kept in the usual course of business.
- Organized and labeled to correspond with the RFP.

(FRCP 34(b)(2)(E)(i).)

If counsel do not understand the organization of the documents they receive, or if the production is overly voluminous, they should ask the producing party for an index of the document production. If the producing party does not provide a sufficient explanation of the documents' organization, the court may compel it to do so (see, for example, *Silicon Storage Tech., Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh, PA.*, 2015 WL 4347711, at *5-6 (N.D. Cal. July 15, 2015); *Lutzeier v. Citigroup Inc.*, 2015 WL 430196, at *8 (E.D. Mo. Feb. 2, 2015); *Century Jets Aviation LLC v. Alchemist Jet Air LLC*, 2011 WL 724734, at *3 (S.D.N.Y. Feb. 8, 2011) (the responding party must provide some information about the organization of documents in its ordinary course of business); *Google, Inc. v. Am. Blind & Wallpaper Factory, Inc.*, 2006 WL 5349265, at *4 (N.D. Cal. Feb. 8, 2006) (responding party must organize and label documents maintained in the ordinary course of business)).

The Producing Party Objects to the Place for Inspection and Copying of Documents

Although no longer that common, an RFP may identify the place for the inspection and copying of documents. The producing party may object to that location on the grounds that it is not reasonable. When the parties dispute the location for inspection and copying, courts look at the burdens and costs to the parties, including:

- The volume of documents for inspection.
- Difficulties getting the documents to the requested location due to high:
  - shipping costs; or
  - copying costs.

(See, for example, *Williams v. Taser Int'l, Inc.*, 2006 WL 1835437, at *6 (N.D. Ga. Jun. 30, 2006).)

The Producing Party Files a Motion for a Protective Order

In response to an RFP, the producing party may decide not to produce documents and instead move for a **protective order** under FRCP 26(c). A court may issue a protective order to protect a party from discovery that annoys, embarrasses, harasses, or imposes an undue burden on it.

The parties must meet and confer to try to resolve the producing party's concerns before the producing party moves for a protective order (FRCP 26(c)(1)). If, after conferring in good faith, the parties cannot agree about the production of certain documents, the producing party may move for a protective order.

There is no automatic stay of discovery while a motion for a protective order is pending. To prevent the producing party from using a motion for a protective order as an end-run to avoid all discovery, counsel should remind the producing party of its obligation to produce responsive documents not subject to the motion for a protective order, both in negotiations with the producing party and in their response to the motion for a protective order.

The Producing Party Withholds Information

The producing party may withhold all or a portion of a document that is responsive to an RFP. This section discusses when the producing party:

- Produces documents with **redacted** content (see The Documents Contain Redacted Content).
- Withholds documents based on claims of **attorney-client privilege** or protected **work product** (see The Producing Party Withholds Documents on Claims of Privilege).

The Documents Contain Redacted Content

Parties sometimes produce documents with redactions (partly sealed contents) so that they produce only relevant, non-privileged information to other parties in the case. This section discusses:

- How to determine the reason for the redactions (see Determining Why The Producing Party Redacted Material).
- When redactions are appropriate (see Appropriate Redactions).

Determining Why the Producing Party Redacted Material

When the producing party redacts material from a document, its counsel should indicate the reason for the redaction (such as "confidential" or "privileged") on the document at the location of the redaction.

If counsel redacts documents to protect attorney-client privileged material, protected work product, or any other privileged material, counsel should identify those documents and describe the nature of the privilege in a **privilege log** (FRCP 26(b)(5)). If the producing party fails to provide a basis for each privilege claim raised, it may waive the asserted privilege (*Culinary Foods, Inc. v. Raychem Corp.*, 1994 WL 48608, at *1, 3 (N.D. Ill. Feb. 16, 1994); see also *Davis v. Hunt Leibert Jacobson P.C.*, 2016 WL 3349629, at *4 (D. Conn. June 10, 2016) (compelling the defendant to produce non-redacted versions of all redacted documents that were not listed on the privilege log); *Micillo v.*

Liddle & Robinson LLP, 2016 WL 2997507, at *3 (S.D.N.Y. May 23, 2016); *SEC v. Yorkville Advisors, LLC*, 300 F.R.D. 152, 167-68 (S.D.N.Y. 2014) (collecting cases) (a party's unjustified failure to timely and properly provide a privilege log operates as a waiver of any applicable privilege)).

Appropriate Redactions

The producing party may redact documents to protect certain information from disclosure, including:

- Privileged material (see generally *U.S. Equal Employment Opportunity Comm'n v. Dolgencorp, LLC*, 2015 WL 2148394, at *2 (N.D. Ill. May 5, 2015); *Kirsch v. Brightstar Corp.*, 2014 WL 4560978, at *3 (N.D. Ill. Sept. 11, 2014); *Schiller v. City of New York*, 244 F.R.D. 273, 274 (S.D.N.Y. 2007)).
- Irrelevant information (see *Byard v. Verizon W. Virginia, Inc.*, 2013 WL 30068, at *15 (N.D.W. Va. Jan. 2, 2013); *Spano v. Boeing Co.*, 2008 WL 1774460, at *3 (S.D. Ill. Apr. 16, 2008) (permitting redaction of information that is not relevant to the case); but see *U.S. ex rel. Simms v. Austin Radiological Ass'n*, 292 F.R.D. 378, 387 (W.D. Tex. 2013) (permitting redactions only for privilege and certain other information); *In re State St. Bank & Trust Co. Fixed Income Funds Inv. Litig.*, 2009 WL 1026013, at *1 (S.D.N.Y. Apr. 8, 2009) (directing certain irrelevant information to remain unredacted)).
- Personal identifiers under FRCP 5.2 (see, for example, *Hale v. State Farm Mut. Auto. Ins. Co.*, 2014 WL 6673550, at *2 (S.D. Ind. Nov. 24, 2014); *Dupuie-Jarbo v. Twenty-Eighth Dist. Court*, 2010 WL 2813343, at *1 (E.D. Mich. Jul. 14, 2010); see also Practice Note, Filing Documents in Federal District Court: Redact Personal Identifiers before Filing).

The Producing Party Withholds Documents on Claims of Privilege

When a producing party claims a document contains privileged material, it must expressly make that assertion and describe the withheld information so that the requesting party can assess the merits of the privilege claim (FRCP 26(b)(5)(A)). Although not specifically mentioned in the FRCP, parties usually comply with this requirement by serving the requesting party with a privilege log. This section discusses when a party may waive its privilege claims because the party:

- Did not timely serve the privilege log (see The Producing Party Did Not Produce the Privilege Log Timely).
- Serves an insufficient privilege log (see The Privilege Log Is Insufficient Overall).
- Logged documents that do not warrant protection from disclosure (see Challenging Specific Documents).

The Producing Party Did Not Produce the Privilege Log Timely

Courts have different rules about when the producing party must serve its privilege log. Depending on the court, counsel may need to serve the privilege log at the time the RFP response is due (see, for example, S.D.N.Y. and E.D.N.Y. L. Civ. R. 26.2(b) (requiring counsel to serve the privilege with the discovery, unless otherwise ordered by the Court)). However, courts do not rigidly enforce this rule (see, for example, *Foster v. City of New York*, 2016 WL 524639, at *5-6 (S.D.N.Y. Feb. 5, 2016); *Williams v. Bridgeport Music, Inc.*, 300 F.R.D. 120, 124 (S.D.N.Y. 2014); *In*

re Chevron Corp., 749 F. Supp. 2d 170, 181 (S.D.N.Y. 2010) aff'd sub nom. *Lago Agrio Plaintiffs v. Chevron Corp.*, 409 F. App'x 393 (2d Cir. 2010) (admonishing courts that do not always rigidly enforce Local Rule 26.2(c))).

Other courts allow the producing party to serve the privilege log at some point in time after the RFP response is due (see *Burlington N. & Santa Fe Ry. Co. v. U.S. Dist. Court for Dist. of Mont.*, 408 F.3d 1142, 1149 (9th Cir. 2005)). However, even in these courts, the producing party must serve the privilege log within a **reasonable** time. Courts determine reasonableness on a case-by-case basis (see, for example, *Best Buy Stores, L.P. v. Manteca Lifestyle Ctr., LLC*, 2011 WL 2433655, at *8 (E.D. Cal. Jun. 14, 2011) (collecting cases); see also *Micillo*, 2016 WL 2997507, at *3 (three month delay unreasonable); *Tatung Co., Ltd. v. Hsu*, 2016 WL 695971, at *10 (C.D. Cal. Feb. 19, 2016) (15 month delay deemed grossly untimely); *Chaplin v. Provident Sav. Bank, FSB*, 2015 WL 502697, at *11 (E.D. Cal. Feb. 5, 2015) (seven month delay not unreasonable); *Carl Zeiss Vision Int'l GmbH v. Signet Armorlite Inc.*, 2009 WL 4642388, at *4 (S.D. Cal. Dec. 1, 2009) (nine month delay not unreasonable); *Horace Mann Ins. Co. v. Nationwide Mut. Ins. Co.*, 240 F.R.D. 44, 48 (D. Conn. 2007) (four month delay unreasonable)).

If the producing party does not produce a privilege log timely, it may waive its privilege claims (see, for example, *Horace Mann Ins. Co.*, 240 F.R.D. at 48).

For more information about when to serve a privilege log, see Standard Document, Privilege Log: Drafting Note: When to Serve the Privilege Log.

The Privilege Log Is Insufficient Overall

Privilege logs give the requesting party an opportunity to assess the producing party's privilege claims. On receipt of a privilege log, counsel should evaluate whether the log generally describes the nature of the documents that the producing party claims are privileged (FRCP 26(b)(5)(A)(ii)). The privilege log is insufficient if it:

- Does not identify the senders or recipients of the documents.
- Lacks a description of the privilege asserted.
- Discloses little information about the contents of the document.

(*Indianapolis Airport Auth. v. Travelers Prop. Cas. Co. of Am.*, 2015 WL 4715202, at *7 (S.D. Ind. Aug. 7, 2015); *Novelty, Inc. v. Mountain View Mktg., Inc.*, 265 F.R.D. 370, 380 (S.D. Ind. 2009); *Williams v. Taser Int'l, Inc.*, 274 F.R.D. 694, 697-98 (N.D. Ga. 2008).)

If the privilege log does not contain sufficient information for counsel to evaluate the validity of the privilege assertions, the producing party may waive the privilege (*In re Grand Jury Subpoena*, 274 F.3d 563, 576-77 (1st Cir. 2001) (upholding privilege waiver for failure to provide a complete privilege log); *Dorf & Stanton Commc'ns, Inc. v. Molson Breweries*, 100 F.3d 919, 923 (Fed. Cir. 1996) (same); *Novelty*, 265 F.R.D. at 381-82 (the plaintiff waived privilege because the privilege log reflected bad faith); *Taser*, 274 F.R.D. at 697-98 (compelling production of documents when the assertions of privilege in the privilege log were wholly inadequate to allow opposing counsel an opportunity to evaluate them)).

For more information about the contents of a privilege log, see Standard Document, Privilege Log: Drafting Note: Privilege Log's Contents.

Challenging Specific Documents

Even if the privilege log is sufficient overall, counsel may challenge privilege claims for specific documents if:

- A description of the claimed protection for any particular document is insufficient.
- An assertion for protection seems improper.

Since privilege waiver is an extreme sanction, a court that finds certain entries deficient may permit the producing party to supplement the privilege log rather than compelling production of the documents identified in the challenged entries.

Counsel Receive Privileged Material

The producing party may inadvertently produce privileged material. This section describes:

- Counsel's obligations on learning that they are in possession of privileged information (see Responding to the Receipt of Privileged Material).
- Whether the inadvertent disclosure results in a waiver of privilege (see Determining Whether the Producing Party Waived the Privilege).

Responding to the Receipt of Privileged Material

Counsel's response to the inadvertent production of documents depends on the circumstances under which they discover the privileged material. Counsel should respond according to:

- FRCP 26 (see Applicability of FRCP 26).
- A confidentiality order entered into by the parties (see The Parties Entered into a Confidentiality Order).
- Ethical rules (see Counsel Identify Privileged Material Without Notice from the Producing Party and Privileged Material Is Included in the Metadata).

Applicability of FRCP 26

FRCP 26 is applicable when the producing party notifies counsel that it inadvertently produced privileged material. If FRCP 26 applies, counsel must:

- Promptly return, destroy, or sequester the privileged material after receiving notice.
- Not use the material until the privilege claim is resolved.
- Not disclose the privileged material.
- Take reasonable steps to retrieve the privileged material already disclosed.

(FRCP 26(b)(5)(B).)

The Parties Entered into a Confidentiality Order

The parties may enter into an order that governs the handling of inadvertently produced privileged documents. For example, they may agree to enter into:

- A confidentiality order (also referred to as a protective order), which may include provisions that:
  - protect against the inadvertent production of privileged information; and
  - set procedures for the return of privileged documents (commonly referred to as a claw-back provision).
- An order under Federal Rule of Evidence (FRE) 502(d).

For more information about confidentiality orders, see Standard Document, Confidentiality Agreement (Order) (Federal).

For more information about claw-back provisions and FRE 502(d) orders, see Practice Note, Attorney-Client Privilege: Waiving the Privilege: Non-Waiver and Clawback Agreements and Court Orders, Standard Document, FRE 502(d) Order, and Standard Clause, Privilege Waiver Clause with Claw-Back Provision.

Counsel Identify Privileged Material Without Notice from the Producing Party

The federal rules do not require counsel to notify the producing party if they receive privileged material that they believe was produced by mistake. However, if there is a confidentiality order in place, counsel must abide by its terms for handling inadvertently produced privileged material (see The Parties Entered into a Confidentiality Order).

If there is no confidentiality order, or if the order is silent on the issue of inadvertently produced privileged material, counsel still must comply with their ethical obligations. Under the American Bar Association's (ABA) Model Rules of Professional Conduct (Model Rules), which provide the basis for most states' ethical rules, counsel must promptly **notify** the producing party if they know or reasonably should know that they mistakenly received privileged documents (Model Rule 4.4). However, the Model Rules do not require counsel either to **stop reviewing or return** documents that they believe are privileged after notifying the producing party. If the producing party advises counsel of the inadvertent production, counsel must destroy, sequester, or return the documents at issue under FRCP 26(a)(5)(B). Counsel should check their state's ethical rules to determine their obligations under the applicable rules.

For information about counsel's ethical obligations on receipt of privileged material, see Practice Note, Attorney-Client Privilege: Waiving the Privilege: Ethics Considerations.

Privileged Material Is Included in the Metadata

Hidden document information (**metadata**) produced in discovery may contain sensitive or privileged information. Metadata is searchable, which raises the ethical question of whether it is appropriate for counsel to search an opposing party's metadata for protected, privileged material.

The Producing Party Voluntarily Produced Its Documents Outside of the Attorney-Client Relationship

Disclosure of documents outside of the attorney-client relationship waives the attorney-client privilege and work product protections. The producing party generally waives protection from disclosure if it voluntarily produces protected documents:

- To a third party.
- In connection with a government investigation.

(See, for example, *In re Pac. Pictures Corp.*, 679 F.3d 1121, 1127-28 (9th Cir. 2012) (rejecting theory of selective waiver and holding that disclosure of documents to the government waived the privilege); but see *United States v. Pac. Gas & Elec. Co.*, 2016 WL 3252779, at *5 (N.D. Cal. June 14, 2016) (reasoning that selective waiver did not apply when the government disclosed documents but retained claims of privilege through a protective order); see also generally *In re Qwest Commc'ns Intl Inc.*, 450 F.3d 1179, 1196 (10th Cir. 2006) (analyzing collected cases); *Gruss v. Zwirn*, 2013 WL 3481350, at *9-11 (S.D.N.Y. July 10, 2013) (same).) The Eighth Circuit is the only circuit to apply the selective waiver doctrine to attorney-client privileged communications (*Diversified Indus., Inc. v. Meredith*, 572 F.2d 596, 611 (8th Cir. 1977)). The Fourth Circuit is the only circuit that has applied selective waiver to opinion work product (see *In re Martin Marietta Corp.*, 856 F.2d 619, 623, 626 (4th Cir. 1988)).

For more information about waiving the attorney-client privilege by disclosing the privileged information to a person outside of the attorney-client relationship, see Practice Note, Attorney-Client Privilege: Waiving the Privilege: Intentional Express Waiver.

Whether to Inspect or Produce Responsive Documents

An RFP should specify a reasonable time, place, and manner for the inspection of documents (**FRCP 34(b)(1)(B)**). Counsel typically request that the producing party make documents available for inspection or production either within 30 days:

- Of the date of the RFP.
- After the parties' **Rule 26(f)** conference if counsel delivered the RFP under **FRCP 26(d)(2)**.

Parties often prefer to produce documents rather than providing access for inspection. This minimizes disruption to the client and controls what information that the requesting party can access.

If the producing party does not copy the responsive documents for production, but rather makes them available for inspection, the requesting party may decide to copy all of the documents that are made available. By copying all of the documents, the requesting party keeps confidential its decisions about the relevancy of the documents and, accordingly, the case strategy.

Social Media: What Every Litigator Needs to Know

This Practice Note discusses key issues surrounding social media in various stages of litigation. Specifically, this Note addresses the use and handling of social media in litigation holds, pre-litigation investigation, service, discovery, jury selection, and at trial. This Note also includes a reference guide on popular social media sites.

Contents

As technology progresses and sources of **electronically stored information (ESI)** proliferate, **social media** content is a part of the litigation equation that courts and counsel increasingly cannot ignore. Disputes over social media content have arisen in all types of actions in all areas of law.

From the pre-litigation stage through **discovery** and trial, social media content often is critical to a party's claim or defense. It can also pose significant challenges. Counsel must be aware of the potential impact of social media on all phases of litigation, as well as some ethical minefields concerning its use.

S

This Practice Note highlights key issues surrounding social media in litigation, including:

- The use of social media in the early stages of litigation.
- Special considerations for discovery and **authentication** of social media content.
- The role of social media in a jury trial.

For more resources to assist counsel and companies in identifying the legal risks of social media use generally, see Practical Law's Social Media Usage Toolkit.

Early Stages of Litigation

Even before a complaint has been drafted or filed, counsel should consider the potential applications of social media. In particular, social media may be a factor in:

- The parties' obligations to preserve and collect relevant evidence as part of a **litigation hold**.
- The pre-litigation investigation of potential adverse parties, witnesses, and opposing counsel.
- The parties' ability to locate and serve adverse parties.

Preservation

The duty to preserve potentially relevant evidence arises when a party reasonably anticipates litigation, and may arise before an action is filed (see Practice Note, Implementing a Litigation Hold: What Is a Litigation Hold?). This duty applies equally to social media content (see *Congregation Rabbinical College of Tartikov, Inc. v. Village of Pomona*, 138 F.Supp.3d 352, 387-88 (S.D.N.Y. 2015); *Howell v. Buckeye Ranch, Inc.*, 2012 WL 5265170, at *2 (S.D. Ohio Oct. 1, 2012)).

In federal court, once litigation commences, the court's scheduling order may specifically provide for preservation of ESI, which could include social media content (FRCP 16(b)(3)(B)(iii)). The parties' discovery plan under the Federal Rules of Civil Procedure (FRCP) must include any issues regarding preservation of these materials (FRCP 26(f)(3)(C)).

Litigation Holds and Collection

As with other potentially relevant ESI, counsel should not overlook social media content in preservation or collection efforts (see *Caputi v. Topper Realty Corp.*, 2015 WL 893663, at *8 (E.D.N.Y. Feb. 25, 2015) (directing plaintiff to preserve all of her Facebook activity through the litigation's duration); *EEOC v. Original Honeybaked Ham Co. of Ga.*, 2012 WL 5430974, at *1 (D. Colo. Nov. 7, 2012) (likening certain social media content to an "Everything About Me" folder that is voluntarily shared with others); see also *Hawkins v. Coll. of Charleston*, 2013 WL 6050324, at *3 (D.S.C. Nov. 15, 2013); *Reid v. Ingerman Smith LLP*, 2012 WL 6720752, at *1 (E.D.N.Y. Dec. 27, 2012)).

Counsel drafting a litigation hold should consider specifically referencing social media platforms, including any associated and collectable **metadata**, among the potential sources of information that custodians should preserve. Similarly, counsel should consider identifying social media platforms as potential sources of relevant information in any demand letter sent to an adversary requesting preservation of relevant ESI.

Counsel may use printouts, screenshots, or web crawlers to capture, gather, and store static images of social media content. However, counsel should bear in mind that these formats may be inconsistent with the format sought in a **request for production** (document request) or **subpoena**, and may be insufficient for authentication (see Document Requests for Social Media Content and Authenticating Social Media).

Therefore, to collect social media content in preparation for a dispute, litigants should consider engaging an **e-discovery** vendor with appropriate expertise to harness the full range of content and metadata associated with the ESI. For resources on engaging an e-discovery vendor, see E-Discovery Toolkit.

Spoliation and Exposure to Sanctions

Digital realities increase the risk that a party or its counsel may be accused of **spoliation** by destroying or altering evidence. This is in part because not all clients appreciate the potential exposure to spoliation sanctions, given how easy it can be to delete, alter, or eliminate a digital file or social media post. Counsel should specifically instruct clients not to destroy or alter social media content where it may be relevant to an anticipated or ongoing litigation.

In federal court, absent an independent tort claim for spoliation under state law, FRCP 37(e) governs the imposition of sanctions or curative measures on a party who fails to take reasonable steps to preserve ESI that should have been preserved and over which the party has control (FRCP 37(e) and 2015 Advisory Committee Notes to FRCP 37(e)). If the lost ESI cannot be restored or replaced through additional discovery, the court may:

- Order measures no greater than necessary to cure any prejudice to another party from the loss of the ESI.
- Upon finding that the party who lost the ESI intended to deprive another party of the ESI's use in the litigation:
  - presume the lost information was unfavorable to the party;
  - instruct the jury that it may or must presume the information was unfavorable to the party; or
  - dismiss the action or enter a default judgment.

(FRCP 37(e)(1), (2). For more information on sanctions under FRCP 37(e), see Practice Note, Sanctions for ESI Spoliation: Overview.)

Counsel therefore should not instruct or suggest to their clients that they intentionally alter, destroy, or disable social media content, because it puts both counsel and the client at risk for severe sanctions.

For more information on key issues that companies and their counsel must consider to ensure compliance with their obligations to preserve and produce ESI, see Practice Notes, E-Discovery in the US: Overview and Practice Note, Practical Tips for Preserving ESI. For more on preserving documents and implementing a litigation hold generally, see Litigation Hold Toolkit. For a sample letter requesting that an opposing or third party preserve relevant evidence and information, see Standard Document, Document Preservation Letter (Demand).

Pre-Litigation Investigation

The investigation of social media content can be highly effective to:

- Help develop a case.
- Frame potential causes of action.
- Resolve a dispute before reaching full-blown discovery.
- Create leverage for settlement.

When preparing a complaint or conducting due diligence in anticipation of litigation, counsel should, at a minimum, conduct internet and social media research on:

- The subject matter of the case.
- Potential parties.

- Opposing counsel.
- Potential witnesses.

However, before searching the social media content of a potential adversary or witness, counsel must understand:

- The applicable ethics rules for conducting pre-litigation investigation.
- How a user's privacy settings may impact the mechanics or ethics of pre-litigation investigation.

Ethical Considerations

Many state and city bar associations have issued ethical guidelines and opinions on the appropriate ways to access social media content. Typically, these guidelines and opinions stem from the basic prohibition on directly or indirectly contacting a represented party absent consent from that party's lawyer under the American Bar Association (ABA) Model Rules of Professional Conduct (ABA Model Rule 4.2).

A lawyer investigating a case generally:

- May access the public portions of a party's or witness's social media account, regardless of whether the party or witness is represented (see, for example, New York State Bar Ass'n (NYSBA) Social Media Ethics Guidelines (2017 NYSBA Guidelines), No. 4.A).
- May **not** access private or non-public portions of a **represented** party's or witness's social media account if the lawyer is required to "friend" or "follow" the account or account user.
- May "friend" or "follow" an unrepresented party or a witness on social media if the lawyer does not engage in deceptive behavior.

Social media content typically is deemed public if information on a person's account is available to anyone without the need for the account holder's permission. This includes content available to all members of a social media network and content that is accessible without authorization to non-members (see, for example, NYSBA Committee on Professional Ethics Op. No. 843 (Sept. 10, 2010)).

Using deception to "friend" or "follow" an unrepresented individual is uniformly deemed unethical, based on either or both:

- ABA Model Rule 4.1, which prohibits a lawyer from making a false statement of (or failing to disclose a) material fact to a third person.
- ABA Model Rule 8.4(c), which states that it is professional misconduct for a lawyer to engage in conduct involving dishonesty, fraud, deceit, or misrepresentation.

However, the interpretation of deception differs across jurisdictions.

In some jurisdictions, including New York, a lawyer can join a social network and connect with or "friend" an unrepresented individual without disclosing the reasons for the request if it does not involve any type of trickery. The lawyer cannot, for example, create a different or false name or profile to mask his identity (see 2017 NYSBA Guidelines, No. 4.B; New York City Bar Ass'n (NYCBA) Committee on Professional Ethics Formal Op. 2010-2, Obtaining Evidence from Social Networking Websites); see also The Sedona Conference® Primer on Social Media, at 57 (Oct. 2012) ("it may be a violation of the Rules of Professional Conduct for a lawyer to request greater access to a user's account under pretext, without being forthright about the request and fully disclosing the purpose of the request")). The lawyer must use her full name and an accurate profile.

Other states require a lawyer to affirmatively disclose her role in a dispute or litigation and identify the client and matter, reasoning that the failure to do so is an omission of a material fact and thereby amounts to deceptive conduct (see N.H. Bar Ass'n Ethics Committee Advisory Op. No. 2012-13/05 BA, Social Media Contact with Witnesses in the Course of Litigation;

San Diego County Bar Ass'n Legal Ethics Op. 2011-2).

Some bar associations go further, requiring attorneys to inform the social media account holder of the intended use of the information, whether generally for litigation or specifically to impeach a witness (see Philadelphia Bar Ass'n Professional Guidance Committee, Op. 2009-02 (Mar. 2009), at 3)).

Privacy Settings

Privacy settings are crucial if a potential party or witness seeks to limit pre-discovery access to ESI. A user's privacy settings often dictate how much information a search may reveal. Therefore, counsel should try to protect a client's social media content from an adversary by maximizing the client's privacy settings. Conversely, an investigating lawyer should seek out as much relevant, public social media content as possible, in part because it can form the basis for requiring an adversary to disclose non-public information (see Relevance Considerations).

When advising a client to maximize privacy settings on any social media account, counsel should caution the client against deleting, altering, or disabling content on the account without also adequately preserving the content, or risk sanctions (see Spoliation and Exposure to Sanctions).

The investigating lawyer's own privacy settings are also important in certain circumstances. For example, some social media platforms, such as LinkedIn, do not allow a lawyer to surreptitiously view social media content without first selecting privacy options to make the lawyer anonymous. Without that setting adjustment, LinkedIn will notify the accountholder that his or her profile was viewed. In addition to alerting an adversary or witness to the lawyer's investigative efforts, these notifications have been considered inappropriate and unethical contact when researching a potential jury pool or sitting juror (see 2017 NYSBA Guidelines, Comment to No. 6.B; see also Jury Selection).

Service of Process

Service is an area in which technological advances, including the proliferation of social media platforms, are reshaping procedural law. Over the past decade, many courts have embraced service of process via email, where due process is satisfied and the relevant state or international statutes or treaties allow for it (see, for example, *Fraserside IP LLC v. Letyagin*, 280 F.R.D. 630, 631 (N.D. Iowa 2012); *U.S. Commodity Futures Trading Comm'n v. Rubio*, 2012 WL 3614360, at *3 (S.D. Fla. Aug. 21, 2012); but see *Joe Hand Promotions, Inc. v. Shepard*, 2013 WL 4058745, at *1-2 (E.D. Mo. Aug. 12, 2013)).

Some plaintiffs, when unable to perfect service through traditional means, have sought court approval to serve process using social media platforms such as Facebook and LinkedIn. Under this type of proposal, a plaintiff would send a message via the social media platform, attaching the summons and complaint, which the account holder could access upon logging into the site. Courts have denied these requests to serve process through social media sites for a number of reasons, including:

- Uncertainty surrounding the authenticity of social media accounts, given the potential for duplicate and false accounts (see, for example, *Fortunato v. Chase Bank USA, N.A.*, 2012 WL 2086950, at *2-3 (S.D.N.Y. June 7, 2012)).
- A lack of confidence that a message posted to a social media account is highly likely to reach defendants or satisfy due process requirements, particularly given users' ability to alter or dismantle their alert settings and notification methods (see, for example, *Miller v. Native Link Constr., L.L.C.*, 2016 WL 247008 (W.D. Pa. Jan. 21, 2016) (denying motion to serve process through LinkedIn); see also *FTC v. Pecon Software Ltd.*, 2013 WL 4016272, at *8 (S.D.N.Y. Aug. 7, 2013); Legal Update, Reining in Facebook and E-mail Service (discussing cases restricting service of process by email and Facebook)).
- Where state law prohibits substitute service by electronic means on domestic defendants, and thus FRCP 4(e)(1) would prohibit service through Facebook in that state (see *Joe Hand Promotions*, 2013 WL 4058745, at *1-2).

However, some courts have allowed service of process via social media as an alternative method of service, particularly where defendants appear to have recently accessed and updated their social media accounts (see, for example, *St. Francis Assisi v. Kuwait Finance House*, 2016 WL 5725002 (N.D. Cal. Sept. 30, 2016); *Ferrarese v. Shaw*, 164 F. Supp. 3d 361 (E.D.N.Y. 2016); *Lipenga v. Kambalame*, 2015 WL 9484473 (D. Md. Dec. 28, 2015); *WhosHere, Inc. v. Orun*, 2014 WL 670817 (E.D. Va. Feb. 20, 2014)).

In light of these cases, litigators seeking to serve via a social media platform should be prepared to:

- Prove the authenticity of related or associated email accounts.
- Demonstrate that the proposed service:
  - is not prohibited by applicable statutes or rules;
  - strictly complies with due process standards; and
  - is highly likely to reach the defendant (for example, by showing that the defendant regularly views and maintains the social media account).
- Serve through email or another method in addition to social media.

Service of Other Documents

Courts have allowed the service of motions and other post-summons documents through Facebook, where Facebook served as a secondary or "backstop" means of service, in addition to email (see, for example, *FTC v. PCCARE247, Inc.*, 2013 WL 841037, at *5 (S.D.N.Y. Mar. 7, 2013) (questioning whether service only by Facebook would comport with due process); see also Legal Update, SDNY: E-mail and Facebook Service on Indian Defendants Approved).

Courts have also permitted widespread notice of class action claims and settlements through social media, although typically counsel must accompany that with another form of notice (see, for example, *In re Nat'l Collegiate Athletic Ass'n Student-Athlete Concussion Injury Litig.*, 2016 WL 305380, at *22 (N.D. Ill. Jan. 26, 2016); *Mark v. Gawker Media LLC*, 2014 WL 5557489, at *4 (S.D.N.Y. Nov. 3, 2014); see also Practice Note, Settling Class Actions: Process and Procedure).

Social Media in Discovery

Once litigation begins, counsel should ensure that discovery efforts cover social media content. Common issues that lawyers must address include:

- Determining whether the user (typically the adversary or a witness) or the social media provider is the right source of the desired ESI.
- Drafting appropriate document requests and **interrogatories** to reach relevant social media content through party discovery.
- Demonstrating the relevance of discovery requests for social media content.
- Responding to discovery requests for social media content.
- Assessing how to authenticate social media content for use in **summary judgment** motions or at trial.

Subpoenas to Non-Party Social Media Providers

Securing production of social media content directly from a provider can be difficult. Some social media providers indicate on their websites or in other official documents that they may produce only limited user or account data or public content, but

not private content, pursuant to a valid federal or state subpoena. These restrictions largely are driven by providers' concerns of running afoul of the **Stored Communications Act** (SCA), which prevents providers of electronic communication services from divulging private communications, and creates a set of statutory "Fourth Amendment-like privacy protections" (18 U.S.C. §§ 2701-2712; *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 971-72 (C.D. Cal. 2010)).

The SCA has been interpreted to cover certain private social media content, such as private messages and non-public posts or comments (see *Crispin*, 717 F. Supp. 2d at 981-82; see also *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 2d 659, 667-68 (D.N.J. 2013) (holding that the SCA protected non-public wall posts on Facebook); *In re Facebook, Inc.*, 923 F. Supp. 2d 1204, 1206 (N.D. Cal. 2012) (quashing a subpoena to Facebook for records from a deceased individual's Facebook account)).

In some cases, for example, Facebook has objected to third-party subpoenas that sought production of a party's social media content because of concerns about the SCA. In these cases, Facebook has suggested that the party download the entire contents of his or her account using the site's "Download Your Information" tool as an alternative method for producing the information. (See *Gatto v. United Air Lines, Inc.*, 2013 WL 1285285, at *2 (D.N.J. Mar. 25, 2013); *In re White Tail Oilfield Servs., L.L.C.*, 2012 WL 4857777, at *2-3 (E.D. La. 2012).) Some courts also have directly ordered parties to use the "Download Your Information" tool and provide a copy of the report to their opponents in response to document requests (see, for example, *Rhone v. Schneider Nat'l Carriers, Inc.*, 2016 WL 1594453, at *3 (E.D. Mo. Apr. 21, 2016)).

For resources on using and responding to subpoenas in federal court generally, see Document Requests and Subpoenas in Federal Court Toolkit.

Document Requests for Social Media Content

Discovery of social media content may be more successful through party discovery. As a best practice, counsel should craft document requests to reach social media content and related metadata by:

- Specifying that the definitions of "document" and "ESI" include social media content. For example:
  - "The term 'document' includes all information published at any time on any site or mobile application, including but not limited to all social networking or social media sites such as Facebook, LinkedIn, Twitter, Instagram, YouTube, or other social media providers."
  - "The term 'ESI' includes all content from social media providers and profiles and all related metadata."
- Including a separate document request that specifically seeks social media content. For example, "All social media postings, comments, messages, or other content relating to the allegations in the Complaint, including but not limited to content from Facebook, LinkedIn, Twitter, Instagram, YouTube, or other social media providers."
- Specifying in the instructions that documents and ESI must be produced with all available metadata. For example, "Electronically stored information ('ESI'), including but not limited to social media content, must be produced and continue to be preserved in its original native format with all relevant metadata, including but not limited to any author, creation date and time, modified date and time, native file path, native file name, and file type."
- Dictating the desired method of production for social media content, whether in native format, paper printouts, or PDF or TIFF formats.

Some courts have required parties to provide log-in and password access to an agent of the court for a pre-production **in camera** inspection of social media content (see, for example, *Original Honeybaked Ham Co.*, 2012 WL 5430974, at *3; *Offenback v. L.M. Bowman, Inc.*, 2011 WL 2491371, at *1 (M.D. Pa. June 22, 2011)). Other courts have relied on user authorizations requesting that the social media provider produce the information (see, for example, *Gatto*, 2013 WL 1285285, at *1).

For a collection of resources on obtaining electronic discovery generally, see E-Discovery Toolkit and Document Discovery Toolkit.

showing that the requested information is relevant, which may be supported by the user's publicly available social media content (see, for example, *Doe v. Rutherford County, Tenn., Bd. of Educ.*, 2014 WL 4080159, at *3 (M.D. Tenn. Aug. 18, 2014) (ordering plaintiffs' counsel to review restricted, nonpublic portions of only one of the plaintiffs' social media accounts and produce relevant information because, based on publicly available social media content, the evidentiary threshold was satisfied only as to that plaintiff); *Keller v. Nat'l Farmers Union Prop. & Cas., Co.*, 2013 WL 27731, at *4-5 (D. Mont. Jan. 2, 2013) (denying a motion to compel absent a threshold showing of relevance, but granting a request for a list of all social networking sites to which the plaintiffs belonged); see also *Potts v. Dollar Tree Stores, Inc.* 2013 WL 1176504, at *3 (M.D. Tenn. Mar. 20, 2013); *Tompkins*, 278 F.R.D. at 388-89).

- Providing detailed guidance on what social media content is relevant to the case and must be produced, including:
  - instructions about the relevance of a party's verbal communications, third-party communications, and photographs and videos to be produced (see, for example, *EEOC v. Simply Storage Mgmt., LLC*, 270 F.R.D. 430, 436 (S.D. Ind. 2010)); and
  - protocols to resolve any disputes on relevance or production (see, for example, *Thompson v. Autoliv ASP, Inc.*, 2012 WL 2342928, at *4-5 (D. Nev. June 20, 2012)).
- Ordering an *in camera* inspection, sometimes in connection with the appointment of a forensic expert special master, to identify relevant social media content from the plaintiffs' accounts (see, for example, *Original Honeybaked Ham Co.*, 2012 WL 5430974, at *2-3; *Offenback*, 2011 WL 2491371, at *1-2).
- Ordering a party's counsel, and not the party, to review the social media content and determine the relevance of the postings (see, for example, *Roberts*, 312 F.R.D. at 608; *Lewis*, 2016 WL 589867, at *3; *Giacchetto*, 293 F.R.D. at 116-17; *Simply Storage*, 270 F.R.D. at 436; *Rutherford Cty. Tenn. Bd. of Educ.*, 2014 WL 4080159, at *3).
- Instructing the requesting party's counsel to review all social media content and inform opposing counsel of relevant information that was not produced, where the existing discovery record suggests that the producing party may have withheld information relevant to the litigation (see, for example, *Thompson*, 2012 WL 2342928, at *5).

Privacy Considerations

In addition to common objections like relevance or undue burden, parties facing discovery requests for social media content often have invoked privacy as a reason to resist disclosure. However, courts generally are dismissive of privacy claims over the public content of social media accounts. The same is usually true for non-public social media content, even where a user has set his privacy settings to shield certain information. Because non-public content is available to select third parties, who may do with it what they wish, courts often reject privacy claims over this information. (See *Lewis*, 2016 WL 589867, at *2; *Chaney v. Fayette Cty. Pub. Sch. Dist.*, 977 F. Supp. 2d 1308, 1315-16 (N.D. Ga. 2013); see also *United States v. Meregildo*, 883 F. Supp. 2d 523, 525-26 (S.D.N.Y. 2012).)

Moreover, where an opponent discovers relevant information from public portions of a party's social media account, a court may be more likely to grant access to non-public content (see, for example, *Rhone*, 2016 WL 1594453, at *2-3 (requiring a plaintiff to provide a "Download Your Information" report from her Facebook account after the defendant discovered relevant information on public portions of her account page)).

However, counsel may attempt to shield non-public social media content through protective orders (see *Finkle v. Howard Cty., Md.*, 2015 WL 3744336, at *8 (D. Md. June 12, 2015), aff'd 2016 WL 878016 (4th Cir. Mar. 8, 2016); *Simply Storage*, 270 F.R.D. at 437; *Ledbetter v. Wal-Mart Stores, Inc.*, 2009 WL 1067018, at *2 (D. Colo. Apr. 21, 2009)).

For more on how to respond to document requests and subpoenas generally, see Practice Notes, Document Responses: First Steps in Responding to an RFP and Subpoenas: Responding to a Subpoena (Federal).

Authenticating Social Media

As with any other type of evidence, social media evidence must be authenticated under FRE 901 to be admissible (see, for example, *United States v. Vayner*, 769 F.3d 125, 126-33 (2d Cir. 2014) (reversing a conviction based on an unauthenticated page of the defendant's alleged profile on a Russian social networking site akin to Facebook)).

Social media evidence may be tangible (such as static screenshots) or consist of ESI, and appropriate methods of authenticating social media vary. For more on general methods of authenticating evidence in federal court, see Practice Note, Evidence in Federal Court: Documents and Other Tangible Evidence Must be Authenticated. For more on authenticating ESI, see Practice Note, E-Discovery: Authenticating Electronically Stored Information and E-Discovery: Authenticating Common Types of ESI Chart, which provides examples of authentication methods for common types of social media.

Because evidence may be authenticated in many ways, federal courts have followed varying approaches to authentication challenges (*Vayner*, 769 F.3d at 133). For example:

- The Third Circuit Court of Appeals held that a defendant's Facebook chat messages, which Facebook gave to the government directly, were authenticated under FRE 901 in part because each of the four witnesses who participated in the chats testified about them, some of the witnesses had met the defendant in person as a result of the chats and could identify him in court, the defendant's testimony showed he owned the Facebook account in question, and biographical information on the page matched that of the defendant (*United States v. Browne*, 2016 WL 4473226, at *6-9 (3d Cir. Aug. 25, 2016); see also *United States v. Barnes*, 803 F.3d 209 (5th Cir. 2015) (Facebook messages were authenticated in part because a witness testified that she had seen the defendant using Facebook and she recognized the account and his style of communicating from the messages)).
- The Fourth Circuit Court of Appeals held that screenshots of Facebook pages and YouTube videos retrieved from a Google server were self-authenticating business records under FRE 902(11) where they were accompanied by certifications from Facebook and YouTube records custodians (*United States v. Hassan*, 742 F.3d 104, 132-34 (4th Cir. 2014); but see *Browne*, 2016 WL 4473226, at *3-6 (Facebook messages were not business records and therefore not self-authenticating under FRE 902(11)).
- The Fifth Circuit Court of Appeals held that photographs on a defendant's Facebook page were not properly authenticated because a "photograph's appearance on a personal webpage does not by itself establish that the owner of the page possessed or controlled the items pictured" (*United States v. Winters*, 530 F. Appx. 390, 395-96 (5th Cir. 2013); see also *Vayner*, 769 F.3d at 131 (the defendant's name, photograph, and some details about his life on a printed profile page was insufficient to establish that he had actually created the profile or was responsible for its contents)).
- The Tenth Circuit Court of Appeals held that Facebook messages were authenticated because the defendant failed to adequately challenge the authenticity of the messages, and the district court had properly admitted the messages as statements of a party opponent at trial (*United States v. Brinson*, 772 F.3d 1314, 1320-21 (10th Cir. 2014)).
- The Eleventh Circuit Court of Appeals held that the district court had properly admitted a YouTube video into evidence because the government presented ample circumstantial evidence through the testimony of various witnesses identifying the individual in the video as the defendant, establishing where and when the video was recorded, and identifying the specific rifle and ammunition in question in the video. Because the government did not make the video, but merely found it on YouTube, it was not required to authenticate the video by offering evidence regarding the integrity of the recording equipment, the competence of the person taking the video, or whether the video was edited. (*United States v. Broomfield*, 591 Fed. App. 847, 851-52 (11th Cir. Dec. 3, 2014).)
- A US district court held that a plaintiff's testimony about photographs posted on an Instagram account and the name associated with the account could authenticate the account, because the plaintiff knew the alleged account holder (*Diperna v. Chicago Sch. of Prof'l Psychology*, 2016 WL 6962836, at *5 (N.D. Ill. Nov. 28, 2016)).
- A US district court held that statements made by a plaintiff on her Facebook page were authenticated by her deposition testimony and admissible as a party admission under Federal Rules of Evidence (FRE) 801(d)(2), 901(a), and 901(b)(1) (*Targonski v. City of Oak Ridge*, 2012 WL 2930813, at *10 (E.D. Tenn. July 18, 2012)).

Counsel should carefully consider authentication issues during discovery, and whether a forensic expert may be needed to authenticate social media evidence. Counsel also should minimize the risk of authentication challenges at the outset of

discovery by proper collection and production of:

- The devices utilized during the creation or use of the social media content.
- Social media metadata (which can be done with the assistance of a vendor or collection software).

(See Preservation.)

Social Media at Trial

Social media can play a large role at trial. As with the investigation of parties, witnesses, and claims, counsel should explore the use of social media when selecting a jury panel. Counsel also should pay attention to the jurors' use of social media during trial and deliberations.

Researching Jurors on Social Media

Counsel can learn important information about prospective jurors, including any potential biases, by examining their:

- Educational and professional backgrounds on sites like LinkedIn.
- "Likes" and followed pages on sites such as Facebook.
- General social media activity, which may indicate whether prospective jurors are likely to seek information about the case outside of the trial record.

However, the parameters for social media investigation are more narrowly applied with respect to jurors and potential jurors than to adverse parties and witnesses (see Pre-Litigation Investigation). For example, the American Bar Association (ABA) issued an opinion:

- Restricting lawyers to searching only the public content of prospective jurors' social media accounts.
- Prohibiting lawyers from connecting with or following a juror or potential juror under any circumstances.

(See ABA Standing Committee on Ethics & Professional Responsibility, Formal Op. 466, Lawyer Reviewing Jurors' Internet Presence (Apr. 24, 2014).)

Given this guidance, lawyers should be cautious with social media platforms like LinkedIn, which may alert a user that his profile and public content have been viewed. This may be interpreted as inappropriate, unethical, and impermissible juror contact. (See NYCBA Committee on Professional Ethics Formal Op. 2012-2, Jury Research and Social Media; see also ABA Model Rule of Professional Conduct 3.5.)

Counsel also should ensure compliance with any specific local or judge's rules or orders applicable to social media research on jurors. At least one court has expressed concern that allowing counsel to conduct social media research on potential and empaneled jurors could facilitate improper personal appeals to particular jurors, compromise the jury verdict, and compromise the jurors' privacy. That court therefore considered exercising its discretion to impose a ban against all internet research on the **venire** or the empaneled jury until the end of trial, a ban to which the parties ultimately agreed. (See *Oracle Am., Inc. v. Google Inc.*, 2016 WL 1252794, at *1-3 (N.D. Cal. Mar. 25, 2016).)

Monitoring Jurors' Use of Social Media

Jurors' misuse of social media during trial is a growing problem that has the potential to undo extensive trial preparation work by resulting in a mistrial or forming the basis for an appeal (see, for example, *United States v. Villalobos*, 2015 WL

544898, at *1-5 (5th Cir. Feb. 11, 2015); *U.S. v. Juror Number One*, 866 F. Supp. 2d 442, 452 n.14 (E.D. Pa. 2011); *In re Methyl Tertiary Butyl Ether (MTBE) Products Liab. Litig.*, 739 F. Supp. 2d 576, 610 n. 215 (S.D.N.Y. 2010) (discussing the "recurring problem" and consequences of social media and internet use by jurors)).

Given the potentially severe consequences, counsel should consider monitoring jurors' use of social media by regularly (and ethically) checking the jurors' social media accounts throughout a trial and deliberations. Although a lawyer who becomes aware of a juror's improper use of social media may be tempted to stay quiet if the juror favors the lawyer's client, some bar associations, including the ABA, require lawyers who observe a juror's misconduct in public social media posts to report it to the court (see ABA Standing Committee on Ethics & Professional Responsibility, Formal Op. 466, Lawyer Reviewing Jurors' Internet Presence (Apr. 24, 2014)).

If jurors' social media use and abuse is a concern or a case is particularly high-profile, counsel may consider asking the court to:

- Instruct the jurors, at multiple points before and during trial, to avoid social media use, and explain the consequences of violating the instruction, such as being held in contempt.
- Require the jurors to take an oath to refrain from social media use during the pendency of the trial.

For examples of jury instructions warning jurors about their use of social media, see *United States v. Feng Ling Liu*, 2014 WL 6076571, at *1-10 (S.D.N.Y. Nov. 14, 2014); *OneBeacon Ins. Co. v. T. Wade Welch & Associates*, 2014 WL 5335362, at *1-11 (S.D. Tex. Oct. 17, 2014); and *Toshiba Corp. v. Imation Corp.*, 2013 WL 7157854, at *10 (W.D. Wis. Apr. 5, 2013).

Counsel Must be Familiar with Popular Social Media Sites

Social media sites can hold a significant amount of relevant ESI and are treasure troves for both informal investigation and formal discovery. Social media websites and platforms connect their users to:

- One another.
- New content (including user-generated content).
- Communication channels that allow for an instant and a permanent online presence.

Many sites also include communication capabilities within their proprietary technologies, such as email, chat, blogging, and others. A common function of most social media sites is the ability for users to post links online for others to see.

To best leverage these rich sources of potentially relevant information, counsel should become familiar with the most popular social media sites, services, and applications. For a description of common categories of social media and a list of currently popular social media services, with non-legal, non-technical descriptions for each, see Practice Note, Social Media: A Quick Guide.

LAW FIRM NAME	**Policy & Procedure**	FUNCTION HIPAA COMPLIANCE
	HIPAA / PRIVACY **FAXING PROTECTED HEALTH INFORMATION**	NUMBER 107
		PRIOR ISSUE 3/1/2015
		EFFECTIVE DATE 3/1/2016

PURPOSE

To ensure that Protected Health Information ("PHI") is appropriately safeguarded when it is sent or received via facsimile (fax) machine or software.

POLICY

It is the policy of this law firm to allow the use of facsimile machines to transmit and receive PHI. The information released will be limited to the minimum necessary to meet the authorized requestor's needs.

PROCEDURE

1. The fax machine is located in an area that is not easily accessible to unauthorized persons. It is monitored by the Program Administrator in the vicinity of the Program Administrator's office. The fax machine is not utilized by unauthorized personnel to ensure confidentiality of PHI is not compromised. A sign is posted regarding access to documents. (See the law firm's sample sign following this Policy.)
2. Received documents will be removed promptly from the fax machine. To promote secure delivery, instructions on the cover page will be followed.
3. As Florida HIPAA law dictates, information transmitted via facsimile is acceptable and may be include the client's PHI to another authorized person and only the minimum necessary to meet the request.
4. Steps that are taken to ensure that the transmission is sent to the appropriate destination. These include:
   a. Pre-programming and testing destination numbers whenever possible to eliminate errors in transmission due to misdialing.
   b. Asking frequent recipients to notify the law firm of a fax number change.
   c. Confirming the accuracy of the recipient's fax number before pressing the send/start key.
   d. Printing a confirmation of each fax transmission.
5. A cover page is attached to any facsimile document sent by the law firm that includes PHI. (See the law firm's sample cover page following this Policy.) The cover page should include:
   a. Destination of the fax, including name, fax number and phone number;
   b. Name, fax number and phone number of the sender;
   c. Date;

d. Number of pages transmitted; and

e. Confidentiality Statement (See sample below).

6. If a fax transmission fails to reach a recipient or if the sender becomes aware that a fax was misdirected, the internal logging system should be checked to obtain incorrect recipient's fax number. A letter will be faxed to the receiver and ask that the material be returned and/or destroyed.

7. A written *Authorization* for any use or disclosure of PHI will be obtained when the use or disclosure is not for service, payment or agency operations or required by federal or state law or regulation.

8. The PHI disclosed will be the minimum necessary to meet the requestor's needs.

9. As dictated by Florida law, highly sensitive health information (e.g., information relating to AIDS/HIV, drug and alcohol abuse, psychiatric treatment, etc.) is only sent by fax with a signed release by the client and the law firm adheres to a client's right of refusal to have this information faxed.

LAW FIRM NAME	**Policy & Procedure**	FUNCTION HIPAA COMPLIANCE
	HIPAA / PRIVACY **FAXING PROTECTED HEALTH INFORMATION**	NUMBER 107
		PRIOR ISSUE 3/1/2015
		EFFECTIVE DATE 3/1/2016

Law Firm's Confidentiality Statement:

The documents accompanying this transmission contain confidential protected health information that is legally privileged. This information is intended only for the use of the individual or entity named above. The authorized recipient of this information is prohibited from disclosing this information to any other party unless required to do so by law or regulation and is required to destroy the information after its stated need has been fulfilled.

If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is strictly prohibited. If you have received this information in error, please notify the sender immediately and arrange for the return or destruction of these documents.

FAX COVER PAGE

Law Firm Name
Address
Phone Numbers (telephone and facsimile)

Confidential and Protected Communication

DATE & TIME _____ NUMBER OF PAGES_____

TO: _____ _____
NAME COMPANY

_____ _____
FAX NUMBER PHONE NUMBER

FROM: _____ _____
NAME COMPANY/LAW FIRM

* Sender's fax number and office number is listed above. *

COMMENTS:

_____

_____

_____

_____

This communication may contain confidential Protected Health Information. This information is intended only for the use of the individual or entity to which it is addressed. The authorized recipient of this information is prohibited from disclosing this information to any other party unless required to do so by law or regulation and is required to destroy the information after its stated need has been fulfilled.

If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or action taken in reliance on the contents of these documents is STRICTLY PROHIBITED by Federal law. ***If you have received this information in error, please notify the sender immediately*** *and arrange for the return or destruction of these documents.*

VERIFICATION OF RECEIPT OF FAX: _____

Only authorized staff may view faxed documents sent or received by this fax machine.

Access to such documents by unauthorized persons is prohibited by federal law.

HIPAA Security Self-Assessment Procedure

HIPAA Security	Safeguard (R) = Required, (A) = Addressable	Status (Complete, N/A)
Administrative Safeguards **LAW FIRM'S procedure to meet the Security Management Process standard in the Security Rule to address security violations by implementing policies and procedures to detect, prevent, contain, and correct these violations include the following steps:**		
Rule Reference	**Procedure and description of how LAW FIRM meets the rule**	
164.308(a)(1)(ii)(A)	LAW FIRM completes the Risk Analysis utilizing IAW NIST Guidelines and the HIPAA Security Rule Toolkit (R)	Reviewed and updated annually or before if needed
164.308(a)(1)(ii)(B)	The Risk Management Process is completed using IAW NIST Guidelines and the HIPAA Security Rule Toolkit (R)	Reviewed and updated annually or before if needed
164.308(a)(1)(ii)(C)	LAW FIRM has instituted a formal sanction policy and procedure and it is utilized against employees who fail to comply with security policies and procedures. These policies and procedures are distributed to and reviewed with all employees. (R)	Distributed and reviewed with employees upon hire. Policy is updated as necessary
164.308(a)(1)(ii)(D)	LAW FIRM has implemented procedures to regularly review records of activity such as audit logs, access reports, and security incident tracking	
164.308(a)(2)	LAW FIRM has assigned security responsibility. The security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity is _____.	The security official was elected upon formation of the company.
164.308(a)(3)(i)	LAW FIRM adheres to Workforce security by implementation of policies and procedures to ensure that all members of workforce have appropriate access to EPHI, and to prevent those workforce members who do not from obtaining access to electronic protected health information (EPHI).	
164.308(a)(3)(ii)(A)	LAW FIRM has implemented procedures for the authorization and/or supervision of employees who work with EPHI or in locations where it might be accessed. (A)	
164.308(a)(3)(ii)(B)	LAW FIRM has implemented procedures to determine if the access of an employee to EPHI is appropriate. (A)	
164.308(a)(3)(ii)(C)	LAW FIRM has implemented procedures for terminating access to EPHI when an employee leaves the organization. (A)	

HIPAA Security	Safeguard (R) = Required, (A) = Addressable	Status (Complete, N/A)
164.308(a)(4)(i)	LAW FIRM addresses information access management by implementing policies and procedures for authorizing access to EPHI that are consistent with the applicable requirements.	
164.308(a)(4)(ii)(A)	LAW FIRM is not a clearinghouse that is part of a larger organization that would require implemented policies and procedures to protect EPHI from the larger organization. (A)	N/A
164.308(a)(4)(ii)(B)	LAW FIRM has implemented policies and procedures for granting access to EPHI through access to a workstation, transaction, program, or process. (A)	
164.308(a)(4)(ii)(C)	LAW FIRM has implemented policies and procedures that are based upon access authorization policies, established, document, review, and modify a user's right of access to workstation, transaction, program, or process. (A)	
164.308(a)(5)(i)	LAW FIRM has addressed security awareness and training by implementing a security awareness and training program for all members of the workforce (including management).	
164.308(a)(5)(ii)(A)	LAW FIRM provides periodic information security reminders. (A)	
164.308(a)(5)(ii)(B)	LAW FIRM has policies and procedures for guarding against, detecting, and reporting malicious software.	
164.308(a)(5)(ii(C)	LAW FIRM has procedures for monitoring log-in attempts and reporting discrepancies. (A)	
164.308(a)(5)(ii)(D)	LAW FIRM has procedures for creating, changing, and safeguarding passwords. (A)	
164.308(a)(6)(i)	LAW FIRM maintains security incident procedures by implementing policies and procedures to address security incidents.	
164.308(a)(6)(ii)	LAW FIRM has procedures to identify and respond to suspected or known security incidents; to mitigate them to the extent practicable, measurable, harmful effects of known security incidents; and to document incidents and their outcomes.(R)	
164.308(a)(7)(i)	LAW FIRM has a Contingency Plan that establish policies and procedures for responding to an emergency or other occurrence (such as fire, vandalism, system failure, or natural disaster) that damages systems that contain EPHI.	
164.308(a)(7)(ii)(A)	LAW FIRM has established and implemented procedures to create and maintain retrievable exact copies of EPHI. (R)	
164.308(a)(7)(ii)(B)	LAW FIRM has established procedures to restore any loss of EPHI data stored electronically. (R)	
164.308(a)(7)(ii)(C)	LAW FIRM has established procedures to enable continuation of critical business processes and for protection of EPHI while operating in the emergency mode. (R)	
164.308(a)(7)(ii)(D)	LAW FIRM has implemented procedures for periodic testing and revision of contingency plans. (A)	
164.308(a)(7)(ii)(E)	LAW FIRM assesses the relative criticality of specific applications and data in support of other contingency plan components. (A)	

HIPAA Security	Safeguard (R) = Required, (A) = Addressable	Status (Complete, N/A)
164.308(a)(8)	LAW FIRM has established a plan for periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of EPHI, that establishes the extent to which LAW FIRM's security policies and procedures meet requirements. (R)	
164.308(b)(1)	LAW FIRM adheres to Business Associate contracts and other arrangements: A covered entity, in accordance with Sec. 164.306, may permit a business associate to create, receive, maintain, or transmit EPHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with Sec. 164.314(a) that the business associate appropriately safeguards the information.	
164.308(b)(4)	LAW FIRM adheres to established written contracts and other arrangements with trading partners that document satisfactory assurances that are required. (R)	
Physical Safeguards		
164.310(a)(1)	LAW FIRM has addressed facility access controls by implementing policies and procedures to limit physical access to electronic information systems and the facility in which they are housed, while ensuring proper authorized access is allowed.	
164.310(a)(2)(i)	LAW FIRM has established procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan. (A)	
164.310(a)(2)(ii)	LAW FIRM has implemented policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. (A)	
164.310(a)(2)(iii)	LAW FIRM has implemented procedures to control and validate a person's access to facilities based on his/her role or function, including visitor control, and control of access to software programs for testing and revision. (A)	
164.310(a)(2)(iv)	LAW FIRM has implemented policies and procedures to document repairs and modifications to the physical components of a facility that are related to security. (A)	
164.310	LAW FIRM has implemented policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access EPHI. (R)	
164.310(c)	LAW FIRM has implemented physical safeguards for all workstations that access EPHI to restrict access to authorized users. (R)	
164.310(d)(1)	LAW FIRM has addressed Device and Media Controls by implementing policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of LAW FIRM, and the movement of these items within LAW FIRM.	

HIPAA Security	Safeguard (R) = Required, (A) = Addressable	Status (Complete, N/A)
164.310(d)(2)(i)	LAW FIRM has implemented policies and procedures to address final disposition of EPHI, and/or hardware or electronic media on which it is stored. (R)	
164.310(d)(2)(ii)	LAW FIRM has implemented procedures for removal of EPHI from electronic media before the media are available for reuse. (R)	
164.310(d)(2)(iii)	LAW FIRM maintains a record of the movements of hardware and electronic media and the person responsible for its movement. (A)	
164.310(d)(2)(iv)	LAW FIRM creates a retrievable, exact copy of EPHI, when needed, before moving equipment. (A)	
Technical Safeguards		
164.312(a)(1)	LAW FIRM addresses Access Controls by implementing technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights as specified in Sec. (a)(4).	
164.312(a)(2)(i)	LAW FIRM has assigned a unique name and/or number for identifying and tracking user identity. (R)	
164.312(a)(2)(ii)	LAW FIRM has established procedures for obtaining necessary EPHI during an emergency.	
164.312(a)(2)(iii)	LAW FIRM has implemented procedures that terminate an electronic session after a predetermined time of inactivity. (A)	
164.312(a)(2)(iv)	LAW FIRM has implemented a mechanism to encrypt and decrypt EPHI. (A)	
164.312(b)	LAW FIRM has implemented audit controls, hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI. (R)	
164.312(c)(1)	LAW FIRM has implemented policies and procedures to protect EPHI from improper alteration or destruction.	
164.312(c)(2)	LAW FIRM has implemented electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner. (A)	
164.312(d)	LAW FIRM has implemented person or entity authentication procedures to verify a person or entity seeking access EPHI is the one claimed. (R)	
164.312(e)(1)	LAW FIRM has addressed Transmission Security by implementing technical security measures to guard against unauthorized access to EPHI being transmitted over an electronic communications network.	
164.312(e)(2)(i)	LAW FIRM has implemented security measures to ensure electronically transmitted EPHI is not improperly modified without detection until disposed of. (A)	
164.312(e)(2)(ii)	LAW FIRM has implemented a mechanism to encrypt EPHI whenever deemed appropriate. (A)	

LAW FIRM NAME

RECORD OF INADVERTENT DISCLOSURE OF PROTECTED INFORMATION

The following information should be entered by the person who inadvertently disclosed, or if unknown, the person who discovered the inadvertent disclosure. Both pages should be provided to the HIPAA Officer after completion.

Covered Component _____ **Date(s) of inadvertent disclosure** _____

Person(s) or entity whose information was disclosed:

Name: _____

ID # or Birth Date (if needed for filing): _____

Address (if known): _____

Phone (if known): _____

Person(s) or entity who received the informati

Name: _____

Address (if known): _____

Phone # (if known): _____

Name: _____

Address (if known): _____

Phone # (if known): _____

The followi fo as a ssed or disclosed (include detail: name, address, health care information, etc.):

_____

_____

(This page to be included in the client record, if covered component is a covered healthcare provider, or should be maintained by the HIPAA Officer in a file of inadvertent disclosures.)

Last Revision 3/25/2017
PREPARED BY:
ASSURED PERSONNEL SOLUTIONS, LLC

V

LAW FIRM NAME
RECORD OF INADVERTENT DISCLOSURE OF PROTECTED INFORMATION

THIS PAGE FOR INTERNAL USE ONLY *(Not to be filed with client record)*

The following information should be entered by the person who inadvertently disclosed, or if unknown, the person who discovered the inadvertent disclosure or disclosed in violation of the minimum necessary. Please include a copy of information disclosed, if reasonable.

Covered Component _____ **Date(s) of inadvertent disclosure** _____

Date disclosure was discovered: _____

Person(s) or entity whose information was disclosed:

Name: _____

ID # or Birth Date (if needed for filing): _____

Person who inadvertently disclosed protected in[illegible]:

Name: _____ **Title:** _____

[illegible]: _____

How was the information inadvertently access[illegible] or [illegible]closed? _____

_____

_____

After the disclosure was discovered, ho[illegible]as the [illegible]ure mitigated?

Confidentiality Agreement [illegible]? Date R[illegible]sted: _____ Date Received: _____

Paper or electronic PHI in cust[illegible]y of the [illegible]ent: D[illegible] Data Requested to be Returned or Destroyed: _____

Date [illegible]turned by Recipi[illegible]: _____ Date Destroyed: _____

Dest[illegible]ion Certif[illegible]te obta[illegible]d? Date Requested: _____ Date Received _____

Other mitigation and how was [illegible] information destroyed, if applicable:

_____

Risk Assessment Data

Please indicate which identifiers were involved in the use or disclosure that relate to the individual or of relatives, employers, or household members of the individual:

Identifier	Individual	Relative	Employer	Household member
Names	☐	☐	☐	☐
Street address, city, county, precinct, zip code	☐	☐	☐	☐

Last Revision 3/25/2017
PREPARED BY:
ASSURED PERSONNEL SOLUTIONS, LLC

LAW FIRM NAME
RECORD OF INADVERTENT DISCLOSURE OF PROTECTED INFORMATION

Dates directly related to an individual, including birth date, admission date, discharge date, date of death	☐	☐	☐	☐
Telephone numbers	☐	☐	☐	☐
Fax numbers	☐	☐	☐	☐
Electronic mail addresses	☐	☐	☐	☐
Social security numbers	☐	☐	☐	☐
Medical record numbers	☐	☐	☐	☐
Health plan beneficiary numbers	☐	☐	☐	☐
Account numbers	☐	☐	☐	☐
Certificate/license numbers	☐	☐	☐	☐
Vehicle identifiers and serial numbers, including license plate numbers	☐	☐	☐	☐
Device identifiers and serial numbers	☐	☐	☐	☐
Web Universal Resource Locators (URLs)	☐	☐	☐	☐
Internet Protocol (IP) address numbers	☐	☐	☐	☐
Biometric identifiers, including finger and voice prints	☐	☐	☐	☐
Full face photographic images and any comparable images	☐	☐	☐	☐
Any other unique identifying number, characteristic, or code	☐	☐	☐	☐

Categories of information disclosed:

Clinical	**Demographics**	**Financial**	**Other**
☐ Diagnosis/Conditions	☐ Address/ZIP	☐ Claims Information	Please list below:
☐ Lab Results	☐ Date of Birth	☐ Credit Card/Bank Acct #	
☐ Medications	☐ Driver's License	☐ Other Financial Information	
☐ Other Treatment Information (list below)	☐ Name		
	☐ SSN		

Is the recipient a covered by HIPAA? (If you are not sure, ask the recipient.) ☐ Yes ☐ No

Name of person completing this form: _____

Signature of person completing this form: _____ **Date:** _____

Phone: _____

The following should be entered by the HIPAA Officer:

How did HIPAA Officer follow up to prevent this incident from recurring?

_____

_____

_____

Last Revision 3/25/2017
PREPARED BY:
ASSURED PERSONNEL SOLUTIONS, LLC

LAW FIRM NAME
RECORD OF INADVERTENT DISCLOSURE OF PROTECTED INFORMATION

Signature of area HIPAA Officer: _____ **Date:** _____

HIPAA Officer: after investigation, all information should be forwarded to the Executive Director/Owner of the Agency and maintained in the HIPAA Officer file. All documents shall be maintained according to HIPAA law.

Last Revision 3/25/2017
PREPARED BY:
ASSURED PERSONNEL SOLUTIONS, LLC

Administrative Compliance

Document ID:

Title: **HIPAA Sanction Policy**

Revision 1.0

Prepared by: Assured Personnel Solutions, LLC

Effective Date: 03/01/17

(775) 335-9648

Policy: It is the policy of LAW FIRM to comply with all federal and state HIPAA Sanction regulations by applying appropriate sanctions against personnel who fail to comply with HIPAA Privacy and Security requirements pertaining to protected information.

Purpose: The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that covered entities have and apply appropriate sanctions against members of their workforce who fail to comply with Privacy Policies and Procedures of the entity, or the requirements of the HIPAA Rule. LAW FIRM will ensure the confidentiality of client protected information as required by law, professional ethics, and accreditation and/or licensure requirements. This policy establishes agency policy, guidance, and standards for workforce performance expectations in carrying out the provisions of HIPAA, and the corrective action(s) that may be imposed to address privacy violations.

Scope: This policy applies to all HIPPA Sanction standards applicable to LAW FIRM. All agency personnel will be governed under this policy and subject to HIPAA Sanctions in the event of a Breach.

Procedure: 1.1 LAW FIRM will provide the necessary resources, staff training, and time to maintain protected information is secure and avoid any type of Breach. All staff will

receive HIPAA training upon hire and will be given the HIPAA Sanction Policy that outlines definition of Breach Class Offenses and the consequences of the HIPAA Disciplinary Sanctions (listed in this policy) that are a result of a Breach.

1.2 All employees will be informed of the HIPAA regulations and of the sanctions for violation of any applicable local, state, or federal law. Employees found to have violated HIPAA disclosure provisions will be disciplined in accordance with LAW FIRM HIPAA Disciplinary Actions up to and including termination of employment. The type of action will depend on the intent of the individual and severity of the violation. The offenses listed below, while not all inclusive, are categorized according to the severity of the violation.

Definition of Offenses

Class I offenses:

Improper and/or unintentional disclosure of data or records. This level of breach occurs when an employee unintentionally or carelessly accesses, reviews or reveals client or employee PHI to himself or others without a legitimate need-to-know. Examples include, but are not limited to:

(1) An employee discusses client information in a public area where the public could overhear the conversation;
(2) An employee leaves a copy of client's protected information in a public area;
(3) An employee leaves a computer unattended in an accessible area with client information unsecured;
(4) An employee accesses information not needed for his/her job;
(5) An employee shares computer access codes (user name and password);
(6) An employee leave computer unattended while logged on with protected information;
(7) An employee shares protected information with another employee without authorization;
(8) An employee copies protected information without authorization;
(9) An employee changes protected information without authorization; or
(10) An employee changes protected information without authorization.

Class II offenses:

Unauthorized use and/or misuse of PHI or records. This level of breach occurs when an employee intentionally accesses or discloses PHI in a manner that is inconsistent with LAW FIRM NAME policies and procedures, but for reasons unrelated to personal gain. Examples include, but are not limited to:

(1) An employee looks up birth dates, addresses, records or relatives;
(2) an employee accesses and reviews the record of a client's out of curiosity or concern;
(3) An employee reviews a public personality's record;
(4) An employee uses or discloses unauthorized protected information;
(5) An employee uses another person's computer access codes (user name and password); or
(6) An employee fails to comply with agency or HIPAA recommendations.

** A second offense of any class I offense (does not have to be the same offense) is a class II offense. **

Class III offenses:

Willful and/or intentional disclosure of PHI or records. This level of breach occurs when an employee accesses, reviews or discloses PHI for personal gain or with malicious intent. Examples include, but are not limited to:

(1) An employee reviews a client record to use information in a personal relationship;
(2) An employee compiles a mailing list for personal use or to be sold.
(3) An employee obtains protected information under false pretenses; or
(4) An employee uses and/or discloses protected information for commercial advantage, personal gain or malicious harm

** A third offense of any class I offense (does not have to be the same offense) or a second offense of a class II offense is a class III offense. **

1.3 LAW FIRM adheres to the HIPAA Disciplinary Sanctions process that will be implemented for any employee HIPAA breach offense (as defined below).

HIPAA Disciplinary Sanctions

Class I offenses shall include, but are not limited to:

(a) Verbal reprimand;
(b) Written reprimand in employee's personnel file;
(c) Retraining on HIPAA Awareness;
(d) Retraining on Company's Privacy and Security Policy and how it impacts the said employee and said employee's department; or
(e) Retraining on the proper use of internal forms and HIPAA required forms.

Class II offenses shall include, but are not limited to:

(a) Written reprimand in employee's personnel file;
(b) Retraining on HIPAA Awareness;
(c) Retraining on HIPAA Privacy Policy and how it impacts the said employee and said employee's department;
(d) Retraining on the proper use of internal forms and HIPAA required forms; or
(e) Suspension of employee (In relation to suspension period: minimum of one (1) day/ maximum of three (3) days).

Class III offenses shall include, but are not limited to:

(a)Termination of employment;
(b) Civil penalties as provided under HIPAA or other applicable Federal/State/Local law; or
(c) Criminal penalties as provided under HIPAA or other applicable Federal/State/Local law.

1.4 LAW FIRM maintains an Administrative Action for Employee Breaches process (as outlined below).

Administrative Action for Employee Breaches

For any breach involving an employee, the Privacy Officer, along with the LAW FIRM OWNERS, will develop and implement an appropriate Plan of Correction, in a timely manner.

The Privacy Officer and OWNERS will conduct an appropriate investigation, commensurate with the level of breach and specific facts. This may include, but is not limited to, interviewing the employee accused of the breach, interviewing other employees or clients and reviewing documentation. Upon conclusion of the investigation, a written report including all findings and conclusions regarding the alleged breach, will be completed. The LAW FIRM OWNERS will make final determination of the appropriate disciplinary action based on the report.

Reporting and Filing Requirements

For all levels of breach, after final resolution the initial report and all supporting documentation will be filed in a confidential file with the Privacy Officer. A copy of the report and supporting documentation will also be placed in the Personnel File of the employee.

All HIPAA investigative documentation will be completed as required. If the employee offense rises to a breach that poses a risk of harm, notification and HHS reporting protocol will be followed (as outlined in the LAW FIRM'S Breach Investigation and Notification Policy).

1.5 LAW FIRM recognizes and abides by sanction exemptions according to law (as outlined below).

Sanction Exemptions

Sanctions will not apply to disclosures by employees who are whistleblowers or crime victims. LAW FIRM is not considered to have violated PHI disclosure requirements if the disclosure is by an employee or business associate as follows:

Disclosure by Whistleblowers

The employee is acting in good faith on the belief that the LAW FIRM has engaged in conduct that is unlawful or otherwise violates professional or clinical standards; or,

That the care, services and conditions provided by LAW FIRM potentially endangers one (or more) clients, employees or a member of the general public; or,

The disclosure is made to a federal or state health oversight agency or public health authority authorized by law to oversee the relevant conduct or conditions of the covered entity; or,

The disclosure is made to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the agency; or

The disclosure is made to an attorney retained by or on behalf of the employee or business associate for the purpose of determining legal options regarding disclosure conduct.

Disclosure by Crime Victims

A covered entity is not considered to have violated the use and disclosure requirements if a member of its workforce who is the victim of a criminal act discloses protected information to a law enforcement official about the suspected perpetrator of the criminal act, and the disclosed protected information is limited to identification and location purposes.

Mitigation

Mitigating circumstances include conditions that would support reducing a sanction in the interest of fairness and objectivity. LAW FIRM will mitigate, to the extent practicable, any harmful effect that is known to be the result of the use or disclosure of protected information in violation of HIPAA regulations.

1.6 LAW FIRM abides by all laws regarding retaliation. No individual will be be subject to any form of retaliation (as outlined below).

Retaliation

LAW FIRM will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against an individual for:

Exercises his rights or participates in the LAW FIRM complaint process; or,

Files a complaint with the Secretary of Health and Human Services; or,

Testifies, assists, or participates in an investigation, compliance review, proceeding or hearing; or,

Opposes any act or practice unlawful under HIPAA, providing that the individual acted in good faith, believing that the practice was unlawful, the manner of opposition is reasonable, and does not involve disclosure of protected information in violation of HIPPA regulations.

BUSINESS ASSOCIATE ADDENDUM

BETWEEN

_____

and

*(Enter Business Name)*_____

Herein after referred to as the "Business Associate"

PURPOSE. In order to comply with the requirements of the Health In...ce Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, and the Healt...rmation Technology fo... Economic and Clinical Health (HITECH) Act of 2009, P... 111-5 this ...endum is hereby adde... and made part of the Contract between the Covered ...y an... Business ...ciate. This Ad...endum establishes the obligations of the Business Asso... and the Co... d Entity as ... as the p...ted uses and disclosures by the Business Associate ...tected healt... ormation it ...pos... by reason of the Contract. The Covered Entity and the Busine... sociate sh... rotect the priv... provide for the security of protected health information disclosed t... Busine... Associate pursua... to the Contract and in compliance with HIPAA, the HIT... ct, and reg... n ...ulgated there under by the U.S. Department of Health and Human Serv... PAA Regula... and other applicable laws.

WHEREAS, the Business Associate will p...ide ...in services ...e Covered Entity, and, pursuant to such arrangement, the Business Associate ...consi...d a busines... sociate of the Covered Entity as defined in HIPAA Regulations; and

WHEREAS, the Busi... iate may have ...cess to a... create, receive, maintain or transmit certain protected healt... rm... om or on b... lf of the C... ed Entity, in fulfilling its responsibilities under such arrangement;

WHEREAS, HIPAA Regulation... uire the C... tity to enter into a contract containing specific require... of the Business As... te prior to the ...closure of protected health information; and

THEREF... E, in ...deration of the ...al obligations below and the exchange of information pursuant to this Add...dum an... tect the inte... of both Parties, the Parties agree to all provisions of this Addendum.

I. DEFINITION... The f...ing ter... his Addendum shall have the same meaning as those terms in the HIPAA Regu... Breach, Data Aggregation, Designated Record Set, Disclosure, Electronic Health Record, Health C... perations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, ...quired by Law, Secretary, Subcontractor, Unsecured Protected Health Information, ...

1. **Business A...ciate** ...hall mean the name of the organization or entity listed above and shall have the meaning given ...he term under the Privacy and Security Rule and the HITECH Act. For full definition refer to 45 CF... 0.103.

2. **Co...** ...ll refer to this Addendum and that particular Contract to which this Addendum is made a part.

3. **Covered Entity** shall mean the name of the Division listed above and shall have the meaning given to such term under the Privacy Rule and the Security Rule, including, but not limited to 45 CFR 160.103.

X

4. **Parties** shall mean the Business Associate and the Covered Entity.

II. OBLIGATIONS OF THE BUSINESS ASSOCIATE

1. **Access to Protected Health Information.** The Business Associate will provide, as directed by the Covered Entity or an individual, access to inspect or obtain a copy of protected health information about the individual that is maintained in a designated record set by the Business Associate or its agents or subcontractors, in order to meet the requirements of HIPAA Regulations. If the Business Associate maintains an electronic health record, the Business Associate, its agents or subcontractors shall provide such information in electronic format to enable the Covered Entity to fulfill its obligations under HIPAA Regulations.

2. **Access to Records.** The Business Associate shall make its internal practices, books and records relating to the use and disclosure of protected health information available to the Covered Entity and to the Secretary for purposes of determining Business Associate's compliance with HIPAA Regulations.

3. **Accounting of Disclosures.** Upon request, the Business Associate and its agents or subcontractors shall make available to the Covered Entity or the individual information required to provide an accounting of disclosures in accordance with HIPAA Regulations.

4. **Agents and Subcontractors.** The Business Associate must ensure that all agents and subcontractors that create, receive, maintain, or transmit protected health information on behalf of the Business Associate agree in writing to the same restrictions and conditions that apply to the Business Associate with respect to such information. The Business Associate must implement and maintain sanctions against agents and subcontractors that violate such restrictions and conditions and shall mitigate the effects of any such violation as outlined under HIPAA Regulations.

5. **Amendment of Protected Health Information.** The Business Associate will make available protected health information for amendment and incorporate any amendments in the designated record set maintained by the Business Associate or its agents or subcontractors, as directed by the Covered Entity or an individual, in order to meet the requirements of HIPAA Regulations.

6. **Audits, Investigations, and Enforcement.** If the data provided or created through the execution of the Contract becomes the subject of an audit, compliance review, or complaint investigation by the Office of Civil Rights or any other federal or state oversight authority, the Business Associate shall notify the Covered Entity immediately and provide the Covered Entity with a copy of any protected health information that the Business Associate provides to the Secretary or other federal or state oversight agency concurrently, to the extent that it is permitted to do so by law. The Business Associate and individuals associated with the Business Associate are solely responsible for all civil and criminal penalties assessed as a result of an audit, breach or violation of HIPAA Regulations.

7. **Breach or Other Improper Access, Use or Disclosure Reporting.** The Business Associate must report to the Covered Entity, in writing, any access, use or disclosure of protected health information not permitted by the Contract, Addendum or HIPAA Regulations by Business Associate or its agents or subcontractors. The Covered Entity must be notified immediately upon discovery or the first day such breach is known to the Business Associate or by exercising reasonable diligence would have been known by the Business Associate in accordance with HIPAA Regulations. In the event of a breach or suspected breach of protected health information, the report to the Covered Entity must be in writing and include the following: a brief description of the incident; the date of the incident; the date the incident was discovered by the Business Associate; a thorough description of the unsecured protected health information that was involved in the incident; the number of individuals whose protected health information was involved in the incident; and the steps the Business Associate or its agent or subcontractor is taking to investigate the incident and to protect against further incidents. The Covered Entity will determine if a breach of unsecured protected health information has occurred and will notify the Business Associate of the determination. If a breach of unsecured protected health information is

determined, the Business Associate must take prompt corrective action to cure any such deficiencies and mitigate any significant harm that may have occurred to individual(s) whose information was disclosed inappropriately.

8. **Breach Notification Requirements.** If the Covered Entity determines a breach of u[n]secured protected health information by the Business Associate, or its agents or subcontractors has oc[cu]rred, the Business Associate will be responsible for notifying the individuals whose unsecured protect[ed] health information was breached in accordance with HIPAA Regulations. The Business Associate [must] provide evidence to the Covered Entity that appropriate notifications to individuals and/or media, w[hen] necessary, as specified in HIPAA Regulations has occurred. The Business Associate is respons[ible] for all cos[ts] associated with notification to individuals, the media or others as well as costs asso[ciated] wi[th] mitigating future breaches. The Business Associate must notify the Secretary of all breaches in a[ccor]dance with HIPAA Regulations and must provide the Covered Entity with a co[py] of all notifications m[ade] to the Secretary.

9. **Data Ownership.** The Business Associate acknowledges that the B[usi]ness Associate or its ag[ents] subcontractors have no ownership rights with respect to t[he] protected he[alth] information it creates, receives or maintains, or otherwise holds, transmits, u[ses] or discloses.

10. **Litigation or Administrative Proceedings.** [The] Business Ass[ocia]te shall m[ake] itself, [its] subcontractors, employees, or agents assisting th[e Bu]siness Assoc[iate] in the perfo[rma]nce of its obligations under the Contract or Addendum, availab[le] to the Cove[red] Entity, at no co[st] to the Covered Entity, to testify as witnesses, or otherw[ise] in the event [of] action[s] or administrative proceedings are commenced against the Covered Entit[y], its administrators or [wo]rkforce members upon a claimed violation by Business Associate of HIPAA Regul[ations] or other laws re[lating] to security and privacy.

11. **Minimum Necessary.** The Business A[ssoci]ate and its agents [or] subcontractors shall request, use and disclose only the minimum amount of p[rote]cted [health] information [ne]cessary to accomplish the purpose of the request, use or disclosure in a[cco]rdance with HIPAA Regulations.

12. **Policies and Proc[edu]res.** Business A[ssoci]ate must [have] written privacy and security policies and procedures and doc[umen]tation standards to m[eet] the requirements of HIPAA Regulations.

13. **Privacy and Security Offi[cer].** The Bu[sine]ss Associate must appoint Privacy and Security Officer[s] whose responsibilities [shall] include: mo[nito]ring the Privacy and Security compliance of the Busines[s Associate]; development a[nd] implementation of the Business Associate's HIPAA Privacy and Security [poli]cies and procedures; esta[blish]ment of Privacy and Security training programs; and developme[nt] and imp[lemen]tation of an i[nci]dent risk assessment and response plan in the event the Business A[ssoci]ate sustai[ns a] breach or su[spe]cted breach of protected health information.

14. **Safeguard[s].** The B[usi]ness Ass[ociate] must implement safeguards as necessary to protect the confidentiality, i[nte]grity and availability of the protected health information the Business Associate creates, receives, [main]tains, or otherwise holds, transmits, uses or discloses on behalf of the Covered Entity. Safeguards [must] include administrative safeguards (e.g., risk analysis and designation of security [offi]cial sa[fe]guards (e.g., facility access controls and workstation security), and technical [safe]guards (e.g., acc[ess] controls and audit controls) to the confidentiality, integrity and availability of the protected hea[lth] inform[ation], in accordance with HIPAA Regulations. Technical safeguards must meet the standards set f[orth] by the guidelines of the National Institute of Standards and Technology (NIST). The Business Asso[ciate] agrees to only use or disclose protected health information as provided for by the Contract and [Ad]dendum and to mitigate, to the extent practicable, any harmful effect that is known to the Busine[ss Asso]ciate, of a use or disclosure, in violation of the requirements of this Addendum as outlined in HIPA[A] Regulations.

15. **Training.** The Business Associate must train all members of its workforce on the policies and procedures associated with safeguarding protected health information. This includes, at a minimum,

training that covers the technical, physical and administrative safeguards needed to prevent inappropriate uses or disclosures of protected health information; training to prevent any intentional or unintentional use or disclosure that is a violation of HIPAA Regulations; and training that emphasizes the criminal and civil penalties related to HIPAA breaches or inappropriate uses or disclosures of protected health information. Workforce training of new employees must be completed within 30 days of the date of h and all employees must be trained at least annually. The Business Associate must maintain n records for a period of six years. These records must document each employee that received tr g and the date the training was provided or received.

16. **Use and Disclosure of Protected Health Information.** The Business Associ ust not r further disclose protected health information other than as permitted or required by ntr as required by law. The Business Associate must not use or further disclose protected he mation in a manner that would violate the requirements of HIPAA Regulation

III. PERMITTED AND PROHIBITED USES AND DISCLOSURES B E BUSINESS ASSOC E
The Business Associate agrees to these general use and disclosure p ions:

1. **Permitted Uses and Disclosures:**

a. Except as otherwise limited in this Addendum Business Ass te may us disclo tected health information to perform functions, activities, vices for, or behalf of, th Entity as specified in the Contract, provided that such use or d sure wou t violate HIPA ulations, if done by the Covered Entity.

b. Except as otherwise limited in this Ad he Busines ociate may use or disclose protected health information received by the Busine As te in its cap as a Business Associate of the Covered Entity, as necessary, for the prop nana ent and ad tration of the Business Associate, to carry out the legal responsibilities of the B ness ciate, as re d by law or for data aggregation purposes in accordance with HIPAA Regulati

c. Except as otherwise ed Addendu the Busi Associate discloses protected health information to a third par e Bus Associa ust obtain, prior to making such disclosure, reasonable written assuran om the rty t such protected health information will be held confidential pursuant to this A dum and ed as required by law or for the purposes for which it disclosed to the thir y. The writt ement from the third party must include require mediately notify usiness Associate of any breaches of confidentiality of protected health in ati extent it has ned knowledge of such breach.

d. The Busi s Associat se or disc e protected health information to report violations of law to appropriate f al and st ies, consistent with HIPAA Regulations.

2. **Prohibited U Disclosures:**

a. Exce as other limited in this Addendum, the Business Associate shall not disclose protected ion to ealth plan for payment or health care operations purposes if the patient has ired thi cial re ction, and has paid out of pocket in full for the health care item or service to which the prot d hea h information relates in accordance with HIPAA Regulations.

b. The Busine ssociate shall not directly or indirectly receive remuneration in exchange for any protected he information, unless the Covered Entity obtained a valid authorization, in accordance with HIPAA tions that includes a specification that protected health information can be exchanged for remuneration.

IV. OBLIGATIONS OF THE COVERED ENTITY

1. The Covered Entity will inform the Business Associate of any limitations in the Covered Entity's Notice of Privacy Practices in accordance with HIPAA Regulations, to the extent that such limitation may affect the Business Associate's use or disclosure of protected health information.

2. The Covered Entity will inform the Business Associate of any changes in, or revocation of, permission by an individual to use or disclose protected health information, to the extent that such changes may affect the Business Associate's use or disclosure of protected health information.

3. The Covered Entity will inform the Business Associate of any restriction to the use or disclosure of protected health information that the Covered Entity has agreed to in accordance with HIPAA Regulations, to the extent that such restriction may affect the Business Associate's use or disclosure of protected health information.

4. *Except in the event of lawful data aggregation or management and administrative activities*, the Covered Entity shall not request the Business Associate to use or disclose protected health information in any manner that would not be permissible under HIPAA Regulations, if done by the Covered Entity.

V. TERM AND TERMINATION

1. **Effect of Termination:**

a. Except as provided in paragraph (b) of this section, upon termination of this Addendum for any reason, the Business Associate will return or destroy all protected health information received from the Covered Entity or created, maintained, or received by the Business Associate on behalf of the Covered Entity that the Business Associate still maintains in any form, and the Business Associate will retain no copies of such information.

b. If the Business Associate determines that returning or destroying the protected health information is not feasible, the Business Associate will provide to the Covered Entity notification of the conditions that make return or destruction infeasible. Upon a mutual determination that return or destruction of protected health information is infeasible, the Business Associate shall extend the protections of this Addendum to such protected health information and limit further uses and disclosures of such protected health information to those purposes that make the return or destruction infeasible, for so long as the Business Associate maintains such protected health information.

c. These termination provisions will apply to protected health information that is in the possession of subcontractors, agents or employees of the Business Associate.

2. **Term**. The term of this Addendum shall commence as of the effective date of this Addendum herein and shall extend beyond the termination of the contract and shall terminate when all the protected health information provided by the Covered Entity to the Business Associate, or accessed, maintained, created, retained, modified, used, stored or otherwise held, transmitted, used or disclosed by the Business Associate on behalf of the Covered Entity, is destroyed or returned to the Covered Entity, or if it is not feasible to return or destroy the protected health information, protections are extended to such information, in accordance with the termination.

3. **Termination for Breach of Contract.** The Business Associate agrees that the Covered Entity may immediately terminate the Contract if the Covered Entity determines that the Business Associate has violated a material part of this Addendum.

VI. MISCELLANEOUS

1. **Amendment.** The parties agree to take such action as is necessary to amend this Addendum from time to time for the Covered Entity to comply with all the requirements of HIPAA Regulations.

2. **Clarification.** This Addendum references the requirements of HIPAA Regulations, as well as amendments and/or provisions that are currently in place and any that may be forthcoming.

3. **Indemnification.** Each party will indemnify and hold harmless the other party to this Addendum from and against all claims, losses, liabilities, costs and other expenses incurred as a result of or arising directly or indirectly out of or in conjunction with:

a. Any misrepresentation, breach of warranty or non-fulfillment of any undertaking on the part of the party under this Addendum; and

b. Any claims, demands, awards, judgments, actions, and proceedings made by any person or organization arising out of or in any way connected with the party's performance under this Addendum.

4. **Interpretation**. The provisions of this Addendum shall prevail over any provisions in the Contract that any conflict or appear inconsistent with any provision in this Addendum. This Addendum and the Contract shall be interpreted as broadly as necessary to implement and comply with HIPAA Regulations. The parties agree that any ambiguity in this Addendum shall be resolved to permit the Covered Entity and the Business Associate to comply with HIPAA Regulations.

5. **Regulatory Reference.** A reference in this Addendum to HIPAA Regulations means the sections as in effect or as amended.

6. **Survival**. The respective rights and obligations of Business Associate under Effect of Termination of this Addendum shall survive the termination of this Addendum.

IN WITNESS WHEREOF, the Business Associate and the Covered Entity have agreed to the *terms of the above written Agreement as of the effective date set forth below.*

COVERED ENTITY	**BUSINESS ASSOCIATE**
(Business Name)	(Business Name)
(Business Address)	(Business Address)
(City, State and Zip Code)	(City, State and Zip Code)
(Business Phone Number)	(Business Phone Number)
(Business Fax Number)	(Business Fax Number)

(Authorized Signature)

(Printed Name)

(Authorized Signature)

(Printed Name)

ess Name)

(Business Address)

(City, State and Zip Code)

(Business Phone Number)

(Business FAX Number)

(Authorized Signature)

(Print Name)

(Date

SECURITY RISK ANALYSIS REPORT

LAW FIRM NAME

SUBMITTED TO:

ALL MEMBERS OF THE RISK ANALYSIS TEAM
COPY MAINTAINED IN CENTRAL FILE FOR REVIEW

SUBMITTED DATE:
3/1/2017

PREPARED BY:
ASSURED PERSONNEL SOLUTIONS, LLC
(775) 335-9648

Table of Contents

I) Executive Summary

LAW FIRM NAME recognizes the best, most up-to-date information is without value unless it is pertinent and accessible to the people it is meant to serve. The Risk Analysis Team has been tasked to conduct a security risk analysis (risk analysis) of LAW FIRM NAME. This Risk Analysis Report summarizes the risk assessment completed. Completing the risk assessment offered us the opportunity to assess the vulnerabilities that are exploited by threats internal and external to LAW FIRM NAME.

The scope of this risk analysis effort was limited to the security controls applicable to LAW FIRM NAME and the environment relative to its conformance with the Health Information Portability and Accountability Act of 1996 (HIPAA) and Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH). These minimum security requirements address general security controls in the areas of policies, procedures, computer hardware and software, client data, operations, administration, management, information, LAW FIRM NAME communication, personnel, and contingency. The purpose of this risk assessment was to identify conditions where Electronic Protected Health Information (ePHI) could be disclosed without proper authorization, improperly modified, or made unavailable when needed. This information is then used to make risk management decisions on whether current safeguards are sufficient, and if not, what additional actions are needed to reduce risk to an acceptable level

This risk analysis was conducted based on many of the methodologies described in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, *Risk Management Guide for Information Technology Systems* (NIST SP 800-30). NIST SP 800-30 uses a nine step process to determine the extent of potential threats and the risk associated with systems. The methodology used to conduct this risk analysis is qualitative, and no attempt was made to determine any annual loss expectancies, asset cost projections, or cost-effectiveness of security safeguard recommendations.

As defined in NIST SP 800-66, a risk is the potential impact that a threat can have on the confidentiality, integrity, and availability of ePHI by exploiting a vulnerability. While it is not possible to be absolutely certain that all risks have been identified, the Risk Analysis Team identified as many as possible known to the organization at the time the assessment was done. This risk analysis identified of ____vulnerabilities: ___were rated **High**, ___were rated **Moderate**, and ___were rated as **Low**. Vulnerabilities are weaknesses that may be exploited by a threat or group of threats. These vulnerabilities can be mitigated by taking measures to implement the recommended actions/controls (safeguards). Safeguards are security features and controls that, when added to or included in the information technology environment, mitigate the risk associated with the operation to manageable levels. A complete discussion of the vulnerabilities and recommended safeguards are found in the HIPAA Risk Assessment.

LAW FIRM NAME recognizes that if the safeguards recommended in this risk analysis are not implemented, the result could be modification or destruction of data, disclosure of sensitive information, or denial of service to the users who require the information on a frequent basis. LAW FIRM NAME is committed to addressing mitigating any and all vulnerabilities.

II) Introduction

A) *Purpose*

The purpose of this risk analysis performed by LAW FIRM NAME, based on compliance with HIPAA and HITECH related security requirements, is to evaluate the adequacy of LAW FIRM NAME's security controls. This risk analysis provides a structured qualitative assessment of the operational environment. It addresses threats, vulnerabilities, risks, and safeguards. The assessment recommends cost-effective safeguards to mitigate threats and associated exploitable vulnerabilities.

B) *Scope*

1) The scope of this risk analysis assesses the system's use of resources and controls (implemented or planned) to eliminate and/or manage vulnerabilities exploitable by threats internal and external to the LAW FIRM and clients' electronic protected health information (ePHI). If exploited, these vulnerabilities could result in:
   (a) Unauthorized disclosure of data
   (b) Unauthorized changes to the system, its data, or both
   (c) Temporary or permanent loss or corruption of data
   (d) Denial of service, access to data, or both to authorized end users
   (e) Loss of financial cash flow
   (f) Loss of physical assets or resources
   (g) Noticeable negative affect on the LAW FIRM'S mission, reputation, or interest
   (h) Disruption in continuity of care for clients served

2) This Risk Analysis Report evaluates the ***confidentiality*** (protection from unauthorized disclosure of system and data information), ***integrity*** (protection from improper modification of information), and ***availability*** (loss of access) of the system. Recommended security safeguards will allow management to make decisions about security-related initiatives to implement to reduce or eliminate identified risks.

C) *System Mission*

The process performed by LAW FIRM NAME's Information Technology (IT) system allows for the compilation of client files to facilitate continuity of legal services and collaboration with other authorized personnel to effectively deliver service provision. In addition, LAW FIRM NAME's IT system allows for the electronic billing of legal services as authorized in the client billing agreement. The IT infrastructure permits the daily operational components required for LAW FIRM NAME to perform the tasks needed to maintain the sovereignty of the LAW FIRM while adhering to the security program.

III) Risk Analysis Approach

A) *Methodology*

1) The risk analysis methodology and approach was conducted using guidelines in NIST SP 800-30, *Risk Management Guide for Information Technology Systems*. The assessment is broad in scope and evaluates security vulnerabilities affecting the confidentiality, integrity, and availability of ePHI. The assessment recommends

appropriate security safeguards, permitting management to make knowledge-based decisions about security-related initiatives to implement to reduce or eliminate identified risks. The methodology addresses the following types of controls:

(a) Management Controls: Management of the information technology ("IT") security system and the management and acceptance of risk.

(b) Operational Controls: Security methods focusing on mechanisms implemented and executed primarily by people (as opposed to systems), including all aspects of physical security, media safeguards, and inventory controls.

(c) Technical Controls: Hardware and software controls providing automated protection to the system or applications (technical controls operate within the technical system and applications).

2) This Risk Analysis Approach section details the risk analysis process performed during this effort.

B) *Participants on the Risk Analysis Team*:

1) _____, Security and Privacy Officer
2) _____, Owner and Chief Information Officer
3) _____, ITAdministrator or Risk Manager
4) _____, HIPAA Consultant

C) *Data Collection Phase.*

The data collection and assessment phase included identifying and interviewing key personnel within the organization and conducting document reviews:

1) Interviews focused on the operating environment.
2) Document reviews provided the Risk Analysis Team with the basis on which to evaluate compliance with security policies and procedures

D) *Risk Assessment Tools & Techniques.*

The following tools and techniques were utilized for the risk assessment:

1) Threat and Vulnerability Identification.

(a) The Risk Analysis Team used NIST SP 800-30 as a basis for threat and vulnerability identification. Refer to Appendix A for the Threat Statement, definitions, and Threat Sources considered.

(b) Through the interview process, "most likely" system and location-specific threats and vulnerabilities were assessed. A thorough understanding of the current security controls (technical & nontechnical) in place for LAW FIRM NAME helps us identify opportunities to reduce the list of vulnerabilities, as well as the realistic probability of a threat attacking ePHI.

(c) Considerations included evaluation of the presence of security incident reports, system break-in attempts, and system down times, if any.

2) Risk Calculation Worksheet: Converts the vulnerabilities into risks based on the following methodology (refer to Appendix B):

(a) Categorizing vulnerabilities

(b) Pairing with threats
(c) Assessing the probability of occurrence and possible impact

3) Risk Level Identification: The Risk Analysis Team determined the degree of risk to the system. Risks were ranked based on risk tolerance and objectives which are important to the LAW FIRM. Vulnerabilities may be identified as individual risks, or may be combined into a single risk based upon likelihood and impact. The determination of risk for a particular threat source was expressed as a function of the following:
   (a) Likelihood Determination: The following factors were considered when calculating the likelihood that a vulnerability might be exploited by a threat (refer to Appendix C for likelihood determination definitions used):
      (i) Threat source motivation and capability
      (ii) Type of vulnerability (flaw or weakness)
      (iii)Existence and effectiveness of current controls
   (b) Impact Analysis: The impact of a security event is the loss or degradation of any, or a combination of any, of the following three security goals, based on successful exploitation of a vulnerability (refer to Appendix C for impact determination definitions):
      (i) Loss of Confidentiality
      (ii) Loss of Integrity
      (iii)Loss of Availability
   (c) Risk Level Determination: The risk determination levels calculated represent the likelihood, degree, and level of risk to which an IT system, LAW FIRM NAME, or procedure might be exposed if a given vulnerability were exercised (refer to Appendix B for risk level definitions).
4) Risk Mitigation: After reviewing identified risks, a risk mitigation action plan was developed. Refer to Appendix D for recommended NIST Risk Mitigation Methodology Activities.

IV) System Characterization (Step 1)

In this step, LAW FIRM NAME's Risk Analysis Team defined the boundaries of the IT system, along with the resources and information that constitute the system, its connectivity, and any other elements necessary to describe the system. Dependencies were clarified. Sensitivity/criticality of the system and data was also determined.

A) *System Contacts & Authorizing Official*

	Business Contact(s) (Responsible for formally accepting each recommended control or providing an alternative)	**Security Official** (HIPAA 164.308(a)(2))	**Authorizing Official(s)** (Authorized to make an informed decision about authorizing the system to operate)
Name			
Title			
Address			
Phone			
E-mail			
IT Systems			

B) *System Related Information*

The Risk Analysis team completed an analysis of the environment by reviewing and updating a Network Diagram as well as an Inventory Asset List. This includes a list of all systems, applications, communication systems, and hardware that store, process, or transmit ePHI and their interdependencies, including billing systems, client files, and administrative documents. These documents are maintained by and may be requested from the Security and Privacy Officer, _____

V) **Threat and Vulnerability Identification** (Steps 2 & 3)

A) *HIPAA Security and HITECH related security requirements Policies and Procedures Risk Assessment*
Refer to the HIPAA Risk Assessment completed on 3/1/2017 which summarizes policies, procedures, safeguards, and controls in place currently used to protect the confidentiality, integrity, and availability of ePHI as required by HIPAA and HITECH. The HIPAA Risk Assessment is maintained by and may be requested from the Privacy and Security Officer, _____

B) *General Threats & Vulnerabilities*
The HIPAA Risk Assessment – Threats document completed on 3/1/2017 includes potential threats and vulnerabilities and the risks associated with each.

VI) **Control Analysis** (Step 4)

Current technical and nontechnical safeguards and controls used are included in the Current State/Comments column of the HIPAA Risk Assessment. Included in the analysis are preventative controls that inhibit attempts to violate security policies, as well as detective controls to warn of violations and attempted violations of security policies.

VII) **Risk Likelihood** (Step 5), **Impact Analysis** (Step 6), & **Determination** (Step 7)

A) The goal of this step is to determine the overall likelihood rating that indicates the probability that a vulnerability could be exploited by a threat-source given the existing or planned security controls, as well as the level of adverse impact that would result from a threat successfully exploiting a vulnerability.
B) The likelihood that a potential vulnerability may happen, the impact that would result from a successful threat exploiting a vulnerability, and the risk determination (level of risk) were determined by using the NIST SP 800-30 Risk Calculation Worksheet in Appendix B and the Risk Likelihood, Risk Impact, and Risk Level Definitions in Appendix C.
C) Refer to the results in the Risk Mitigation Implementation Plan.

VIII) **Summary – Risk Management Recommendations**

A) *Risk Mitigation Strategy*
Risk mitigation involves evaluating, prioritizing, and implementing appropriate safeguards to reduce identified risks during the risk analysis process. The goal is to ensure the confidentiality, integrity, and availability of ePHI.
   1) Because the elimination of all risk is impractical, the LAW FIRM'S Risk Analysis Team will assess control recommendations, determine the acceptable level of residual risk, perform cost-benefit analyses, and approve implementation of those controls that have the greatest risk reduction impact in the most cost-effective manner to meet Security regulation requirements.
   2) Refer to Appendix D for NIST Risk Mitigation Activities, and to NIST SP 800-30 for additional methods to mitigate known and potential risks.

B) *Evaluate and Prioritize Risks*
   1) Safeguarding recommendations are the results of the risk analysis process, and provide a basis by which the HIPAA consultant can evaluate and prioritize the identified risks and LAW FIRM NAME's associated controls.
   2) The Business Contact will work with the Authorizing Official, _____, to develop a Risk Mitigation Implementation Plan, including recommended controls. At this point, the System Contacts can collaborate to either accept the control recommendations or provide alternative suggestions.
      (a) Refer to the Risk Mitigation Implementation Plan in the HIPAA Risk Assessment document for risk mitigation strategies.

(b) The Risk Mitigation Implementation Plan includes risks identified as medium to high priority levels. Low risk priority levels are not included as they are assumed to currently be organizationally accepted risks, but should be evaluated once the medium to high priority risk levels are addressed.

C) *Identify Controls to Mitigate or Eliminate Risks* (Step 8)

1) Controls, safeguarding recommendations, and/or actions that could reduce or eliminate the likelihood and/or impact of the associated risks have been identified and documented in the Risk Mitigation Implementation Plan.
2) The Risk Analysis Team considered all of the following factors when recommending controls and solutions to minimize or eliminate risks (note: these are not in order of importance):
   (a) Sensitivity of the data and the system
   (b) Previous security incidents
   (c) Safety, reliability, and/or effectiveness of controls
   (d) System compatibility and dependencies
   (e) Incompatibilities with other controls
   (f) Legislation and regulations
   (g) Organizational policies and procedures
   (h) Operational impact
   (i) Budgetary constraints
   (j) Other resource constraints

IX) **Risk Mitigation**

A) *Implement Controls*

1) Implement the controls that have been approved and budgeted by LAW FIRM NAME's senior management, or owners, in order of priority (e.g. greatest impact first)
2) Wherever possible, objectively measure the effective reduction in risk as a result of the control, and document this result
3) Identify and resolve unintended problems associated with the control implementation

B) *Ongoing Monitoring*

1) Ongoing monitoring will be done to determine if new risks have developed.
2) Ongoing monitoring includes, but is not limited to, the following:
   (a) Conduct periodic reviews/mini risk assessment of security controls to measure their ongoing effectiveness and document the results.
   (b) Perform periodic system audits/mini risk assessment, such as before upgrading and purchasing new systems, with significant personnel changes, implementing new security policies, etc. When a new or upgraded system is introduced to the organization, a review must be done in order to determine if a new risk analysis must be conducted due to the introduction of new assets in the organization.
   (c) After conducting ongoing risk evaluation mitigate new risks identified.

3) Complete a Risk Analysis/Assessment on a scheduled basis (e.g. every year or as needed to meet LAW FIRM NAME's risk needs, regulatory requirements, and other applicable standards).

X) **Results Documentation** (Step 9)

A) Results of the risk analysis are documented in this report, in the HIPAA Risk Assessment document, and in the Risk Mitigation Implementation Plan.

B) A summary of the Risk Analysis and the Risk Mitigation Implementation Plan will be provided to management and partners (owners) to:
   1) help them understand the risks;
   2) help make decisions on policy, procedure, budget, and system operational and management changes; and
   3) allocate resources to reduce and correct potential and known risks.

C) All risk mitigation strategies and processes will be fully documented, including:
   1) Those that have been approved, budgeted, and implemented
   2) Those that have been approved and budgeted, but not yet implemented
   3) Those that have been approved, but are not yet budgeted
   4) Those that were not approved (including the reason)

D) The above documentation will all be maintained for at least six years by _____, Privacy and Security Officer.

Appendix A: Threat Identification Overview

This information was taken directly from the NIST SP 800-30

Threat Identification Overview

NIST SP 800-30 describes the identification of the threat, the threat source and threat action for use in the risk assessment process. The following is a definition for each:

1. **Threat** – The potential for a particular threat-source to successfully exercise a particular vulnerability. *(A **vulnerability** is a flaw or weakness that can be accidentally triggered or intentionally exploited and result in a security breach or violation of policy).*
2. **Threat Source** – Any circumstance or event with the potential to cause harm to an IT system. The common threat sources can be natural, human or environmental which can impact the LAW FIRM'S ability to protect ePHI.
3. **Threat Action** – The method by which an attack might be carried out (e.g., hacking, system intrusion).

Threat Sources

A threat-source is any circumstance or event with the potential to cause harm to an information technology system and its processing environment. Common threat-sources are natural, human, and environmental. Threat sources can threaten the LAW FIRM'S systems, data, personnel, utilities, and physical operations and how they function, their ability to perform their responsibilities/duties, or exposes them to disruption and/or harm.

Appendix B: Risk Calculation Worksheet & Risk Scale and Necessary Actions

This information was taken directly from the NIST SP 800-30

Risk Calculation Worksheet

The following NIST SP 800-30 calculation worksheet provides instructions for determining the overall risk level for this report. History of past occurrences can help determine the threat likelihood level and impact level can take into account, financial impact, employee safety, and many other factors.

Threat Likelihood	Impact		
	Low (10)	*Medium* (50)	*High* (100)
High (1.0)	Low 10 X 1.0 = 10	Medium 50 X 1.0 = 50	High 100 X 1.0 = 100
Medium (0.5)	Low 10 X 0.5 = 5	Medium 50 X 0.5 = 25	Medium 100 X 0.5 = 50
Low (0.1)	Low 10 X 0.1 = 1	Low 50 X 0.1 = 5	Low 100 X 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)[8]

Risk Scale and Necessary Actions

The following Risk Scale and Necessary Actions table presents actions that NIST SP 800-30 recommends LAW FIRM NAME's senior management (the owners) must take for each risk level.

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, the system's Designated Approving Authority (DAA) must determine whether corrective actions are still required or decide to accept the risk.

Appendix C: Risk Likelihood, Risk Impact, and Risk Level Definitions

This information was taken directly from the NIST SP 800-30

Level	Likelihood Definitions
High (1.0)	The threat source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Moderate (.5)	The threat source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low (.1)	The threat source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

Impact Analysis: The adverse impact of a security event in terms of loss or degradation of any, or a combination of any, of the following three security goals, resulting from successful exploitation of a vulnerability:

- Loss of Confidentiality – Impact of unauthorized disclosure of confidential information (ex. Privacy Act). Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.
- Loss of Integrity – Impact if system or data integrity is compromised by intentional or accidental changes to the data or system.
- Loss of Availability – Impact to system functionality and operational effectiveness should systems be unavailable to end users.

Magnitude of Impact	Impact Definitions
High (100)	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an LAW FIRM'S mission, reputation, or interest.
Moderate (50)	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm or impeded an organization's mission, reputation, or interest.
Low (10)	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources; (2) may noticeably affect an LAW FIRMS' mission, reputation, or interest.

Risk Level Determination: These levels represent the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exercised:

- The likelihood of a given threat source's attempting to exercise a given vulnerability.
- The magnitude of the impact should a threat-source successfully exercise the vulnerability.
- The adequacy of planned or existing security controls for reducing or eliminating risk.

Magnitude of Impact	Risk Level Definitions
High (>50-100)	There is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Moderate (>10-50)	Corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low (1-10)	The system's Authorizing Official must determine whether corrective actions are still required or decide to accept the risk.

Appendix D: NIST Risk Mitigation Methodology Activities

This information was taken directly from the NIST SP 800-30

Input	Risk Mitigation Activities	Output
Risk levels from the risk assessment report	Step 1. Prioritize Actions	Actions ranking from high to low
Risk assessment report	Step 2. Evaluate Recommended Control Options • Feasibility • Effectiveness	List of possible controls
	Step 3. Conduct Cost-Benefit Analysis • Impact of implementing • Impact of not implementing • Associated costs	Cost-benefit analysis
	Step 4: Select Controls	Selected controls
	Step 5: Assign Responsibility	List of responsible persons
	Step 6: Develop Safeguard Implementation Plan • Risks and Associated Risk Levels • Prioritized Actions • Recommended Controls • Selected Planned Controls • Responsible Persons • Start Date • Target Completion Date • Maintenance Requirements	Safeguard implementation plan
	Step 7: Implement Selected Controls	Residual risks