e-Discovery: What Litigation Lawyers Need to Know

RISK MANAGEMENT PRACTICE GUIDE OF LAWYERS MUTUAL

LAWYERS MUTUAL | LIABILITY INSURANCE COMPANY OF NORTH CAROLINA

www.lawyersmutualnc.com

DISCLAIMER: *This document is written for general information only. It presents some considerations that might be helpful in your practice. It is not intended as legal advice or opinion. It is not intended to establish a standard of care for the practice of law. There is no guarantee that following these guidelines will eliminate mistakes. Law offices have different needs and requirements. Individual cases demand individual treatment. Due diligence, reasonableness and discretion are always necessary. Sound risk management is encouraged in all aspects of practice.*

JANUARY 2020

e-Discovery: What Litigation Lawyers Need to Know

Risk Management Practice Guide of Lawyers Mutual

TABLE OF CONTENTS

What is e-Discovery	2
Identification, Preservation, Collection	5
Processing	7
Review	8
Production	9
Conclusion	10
Litigation Hold Notice – Plaintiff	11
Litigation Hold Notice – Defendant	14
Preservation Notice – Third Party	17

LAWYERS MUTUAL LIABILITY INSURANCE COMPANY OF NORTH CAROLINA

919.677.8900 | 800.662.8843 | www.lawyersmutualnc.com

What is E-Discovery?

E-Discovery is discovery involving electronic documents. That's it.

You're probably already doing, or have already done, some type of e-discovery. If your client is emailing documents to your attorney, and your attorney forwards those documents to you to prepare for production, then you are working with e-discovery.

But is this the best approach for dealing with electronic documents?

It depends on the scope of the case. If this is an automobile liability case and your client is emailing you the pictures they took from their phone after the accident occurred, there is probably nothing wrong with this approach. However, if your client is involved in a high dollar business dispute, and a lot of the issues in the case arise around who said what when this is probably not the best approach.

E-Discovery is discovery involving electronic documents. That's it. You're probably already doing, or have already done, some type of e-discovery.

What are some of the pitfalls to this approach?

1. **Completeness**. Did your client actually forward you all the relevant documents? How can you be sure?

2. **Metadata**. If your client is sending you emails by forwarding them to your attorney, the metadata of the underlying emails are lost. What is metadata? In a nutshell, the data surrounding the email: who sent it, who received it, when it was sent, what was attached to it, etc.

3. **And how are you going to keep track of all these documents**? Sometimes, cases start with a client forwarding the ten to twenty most important documents to their attorney. And if your attorney forwards those to you, that may be a fine way to familiarize yourself with key facts. But if opposing counsel requests emails going back seven years, having your client EMAIL all those to your attorney, who then forward them to you – that is a recipe for disaster.

The rules of discovery. Federal Rule 34 requires us to identify which documents are responsive to which requests or produce them as they were kept in the ordinary course of business. In the ordinary course of business, your client likely does not forward your law firm their routine business correspondence. The comments of ABA Model Rule 1.1, which addresses competency, specifically address technology. They state: "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology..." This requires them to at least understand what options you have regarding e-discovery technology. And there are more defensible options than just forwarding via e-mail. Furthermore, if you dive in to the case law across the country, judges are becoming less and less patient with attorneys (and parties) that do not take e-discovery seriously.

So you need a plan. You may not need to use this plan for every new case that comes across your desk, but you will need a plan.

The Electronic Discovery Reference Model ("EDRM") is a great starting point. What is the EDRM? It's an organization that "creates practical resources to improve e-discovery and information governance." You can learn more about the EDRM on their website (www.edrm.net) where they have white papers, guidelines, and more. The site is a little unwieldly, so the standards will be discussed in this practice guide.

This practice guide will focus on specific stages of the EDRM flowchart, which breaks down the different steps required in cases that involve extensive electronic

PRACTICE TIP

ELECTRONIC DISCOVERY REFERENCE MODEL ("EDRM")

IDENTIFICATION. Who are the most important custodians? Where are their documents?

PRESERVATION. Has your client issued a litigation hold?

COLLECTION. How are you going to collect this data?

PROCESSING. Once you have the data, how are you going to look through it? What meta-data do you want pulled out of it?

REVIEW. How are you going to review all these documents? It may be unfeasible to review each documents one-by-one.

PRODUCTION. What are you going to give opposing counsel?

discovery. The flowchart begins with your client's information governance policies and goes all the way through trial presentation.

As we move through the EDRM process, the volume of our data decreases, and the relevance increases. This is represented by the yellow triangle (volume) and green triangle (relevance) in the flowchart. At the beginning you will start with a whole mess of documents. At the end, ideally, you will have honed in on the most relevant documents for production and trial presentation.

In the sections to follow, we will address the stages in the EDRM flowchart:

IDENTIFICATION. Who are the most important custodians? Custodians are simply individuals with relevant data. Where are their documents?

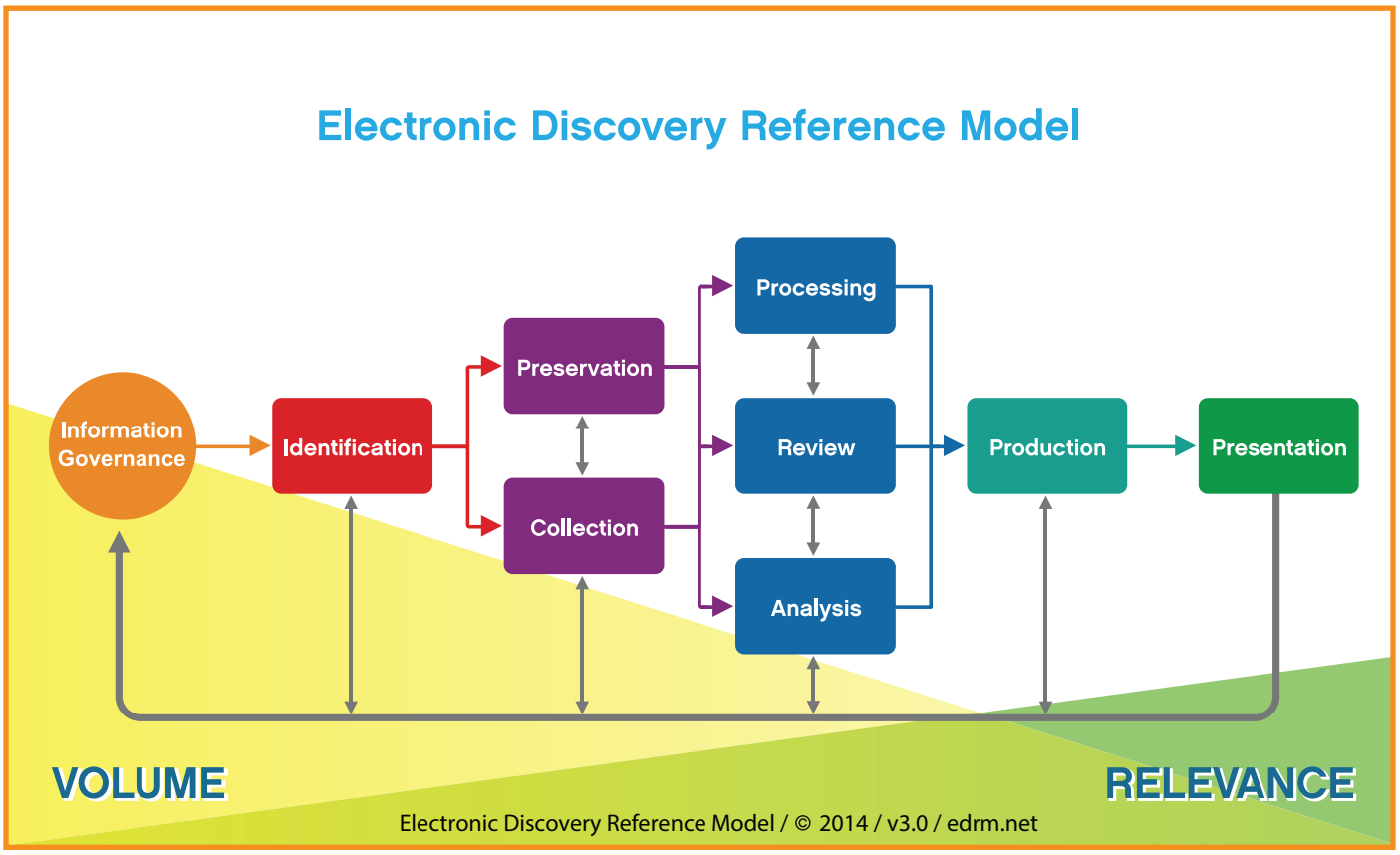
PRESERVATION. Has your client issued a litigation hold?

COLLECTION. How are you going to collect this data?

PROCESSING. Once you have the data, how are you going to look through it? What metadata do you want pulled out of it?

REVIEW. How are you going to review all these documents? It may be unfeasible to review each documents one-by-one.

PRODUCTION. What are you going to give opposing counsel?



IDENTIFICATION, PRESERVATION, COLLECTION

The first phase of your e-discovery plan involves figuring out what documents you need to get and going to get them. Just like any other case, you need documents directly related to the claims and defenses and you need documents requested in discovery.

Identification

Your first step will be to identify who the most relevant custodians are and where their data is kept. A custodian is simply a person/place with relevant data. Keep in mind that a custodian could be a network server or drive! The best way to determine where relevant data resides is to ask your client. Ask about computers, servers, mobile devices, backup tapes, paper files, and more. If you need help developing a list of questions, the EDRM can get you started.

Preservation

While asking your client about the location of their relevant data, you'll also want to ask about your client's information governance policies. This will include, for example, their e-mail deletion policies, what they do with an employee's computer/data when they depart the company, and whether they overwrite back up tapes. You can find sample questions related to records management on the EDRM site. Be aware that your client's information governance policies may be at odds with their duty to preserve (they may have to suspend their e-mail deletion or stop overwriting their back up tapes).

Next you'll need a litigation hold memo informing your client in writing of their duty to preserve relevant documents. This memo should be distributed, by your client, to relevant custodians and IT staff, and will serve to remind them not to delete electronic documents or shred paper documents related to the litigation. A litigation hold memo can be in the form of a memo, a letter, or an e-mail. Several samples can be found on the internet by Googling the term "litigation hold memo." If the litigation spans many years, don't be afraid to follow up with your client; sometimes people forget and employees turn over.

Collection

There are several different options for collection. The EDRM evaluates these different methods and lays out the pros and cons of each. We will focus on the difference between a forensic and a non-forensic collection.

"The first phase of your e-discovery plan involves figuring out what documents you need to get and going to get them. Just like any other case, you need documents directly related to the claims and defenses and you need documents requested in discovery.

A forensic collection is when you preserve all aspects of the document's metadata. This will likely involve a vendor and/or special processing software that copies the entire hard drive or targeted data without altering the metadata.

A non-forensic collection is when you do not preserve all aspects of the document's metadata. Here are some examples:

- Your client copies loose e-documents to a flash drive or uploads them to the cloud. At the least, this alters the dates last modified, dates last accessed, and creation dates.

- Your client forwards you e-mails. This significantly altering the email's metadata – the sender, the recipient, the date sent, and the subject line are all changed.

- Additionally, non-forensic collections may omit folder paths and other custodial information. This metadata can be very helpful for you and is worth preserving!

Why does identification, preservation, and collection matter? The failure to identify, collect, and preserve relevant electronic data can lead to spoliation charges, monetary sanctions, and even an adverse inference instruction

Why does identification, preservation, and collection matter? The failure to identify, collect, and preserve relevant electronic data can lead to spoliation charges, monetary sanctions, and even an adverse inference instruction (because the evidence was not preserved, the jury may infer that the evidence would have been unfavorable to the party responsible for its destruction). You can also lose valuable, helpful data that helps you prove your case!

PRACTICE TIP

OPTIONS FOR COLLECTION OF DATA

FORENSIC COLLECTION. Preserves all aspects of the document's metadata. This would likely involve an outside vendor or software that copies data without altering the metadata.

NON-FORENSIC COLLECTION. This method of collection does not preserve the document's metadata. Examples include:

- Loose documents copied to flash drives and the cloud, This alters the last modified, accessed and creation dates.
- Forwarded emails, which significantly alters the metadata by changing the sender, recipient and subject line .

PROCESSING

After you've collected electronic and hard copy documents from your client, the next stage is processing. Vendors "process" data by extracting the relevant metadata and providing the documents in a more user-friendly format. Vendors can also identify and remove corrupt file or files that may have viruses, weed out junk files or zero byte files, and they can also de-duplicate them (de-dupe) by eliminating exact digital copies. They can also run search terms against your documents (all or a sub-set) to identify the documents most likely to contain relevant information.

> **"Vendors "process" data by extracting the relevant metadata and providing the documents in a more user-friendly format**

Before you approach a vendor to process your data, you need to know the size and format of your data. In terms of size, the vendor will want to know how many megabytes (MB) or gigabytes (GB) of data you have. To determine this, navigate to the folder or device containing your data. Right click the properties and determine the size. The screen shot below shows that the folder "Client Docs" contains 343 files totaling 417 MB. Your vendor is just looking for a ballpark figure, so for this data, I would say we have about 400 files totaling one half of a GB (1 GB = 1000 MB).

Your vendor will also want to know what kind of data you have. There are basically two types of e-documents: emails and loose e-documents. Email files are typically in PST (Microsoft Outlook) or MBOX (corporate or personal Gmail) format. These are compressed files, kind of like zip files of an email account. E-documents are everything else: Microsoft office files, PDFs, photos, videos, specialty files (e.g. AutoCAD drawings, QuickBooks exports).

Prior to processing, you'll need to identify the metadata fields to capture and determine what numbering to use.

For metadata, the E-Discovery reference model provides a standard list of metadata fields and this is a great place to start. You may also want to include the following fields:

BEGATT, ENDATT – These fields connect emails to their attachments. Emails and their attachments are also called families, where the email is the parent document and the attachments are the children. Emails will have field that shows the number of their attachments, and attachments will have a field that shows the number of the email they were attached to.

CUSTODIAN – This identifies who or where the documents they came from. You may need to provide this to your vendor, depending on the collection method.

CODING FIELDS – Coding fields are fields that you will have to fill in yourself. They can't be extracted, because they involve subjective analysis.

- Summary
- Attorney Notes
- Document Description (letter, email, invoice, etc.)
- Responsive Designation
- Privilege Designation and Basis
- Confidentiality level

The vendor will also number the documents during processing. Each document or page will be assigned a unique number for reference. An internal number (or soft number) is just a reference number, like a bates number that's not branded on the document. If you branded your internal number, you would end up with gaps in your production (as non-responsive and privileged documents are removed). An example of an internal number might be: revENRON-000368, with the eventual external number (also called hard number or production number) as ENRON-000008.

REVIEW

When it comes to reviewing your documents, there are many options to choose from. You can purchase document review software that will help expedite your review. If that is simply not an option, you can also conduct your review with a Microsoft Excel spreadsheet and PDF files.

E-Discovery review software is offered by a number of vendors; Catalyst, Concordance, Eclipse, Kroll Ontrack, Relativity, and Summation are just some of the options. Review software comes in a desktop version, which can be purchased for a one-time fee and is downloaded onto your computer, or a web version, which is hosted on the internet. Web-based software is usually hosted and managed by a vendor and can be used on a case-by-case basis. The advantages to review software is that they streamline and expedite your review. The level of efficiency depends on the products and the bells and whistles they offer.

How does this software work? Basically, it captures the document's metadata and image, allowing you to scroll through the images or search on the metadata. They also provide many tagging options, so you can code your documents and type in notes in one portion of the software while you look at the image in another. If you've never seen one before, imagine you have two screens. On one screen is an excel spread sheet. Each document has its own row, with columns containing the metadata. On your second screen is a picture (image) of the document. As you click through the rows on the spreadsheet, the image screen automatically advances.

E-Discovery platforms can also offer analytics (or TAR – technology assisted review) that will help you review your documents more efficiently. These tools can organize your data by concepts using key terms and custodians, or organize e-mail chains so that they can be reviewed together, or predict the relevance of documents in your data set (predictive coding). Predictive coding utilizes a seed set to develop an algorithm and push it across the data set. What does this mean? In very simplistic terms, an attorney reviews 1,000 documents. The software identifies trends in what was marked responsive. It then applies these trends to the rest of the 20,000 data set, and pulls back 7,000 additional documents that it thinks are most similar to the documents marked responsive.

If review software is simply not an option for you, you can use an actual excel spreadsheet and PDF files. It won't be as convenient and you will lose a lot of the searching capabilities, but at least you'll have something! A vendor can extract the metadata into an Excel file and assign an internal number to each document. Then they can create a PDF with the internal number as a title.

PRACTICE TIP

HOW DO YOU REVIEW THE ELECTRONIC DOCUMENTS?

1. Purchase **document review software**

   PROS: Streamline and expedite your review

   CONS: Cost money

2. Conduct your review with a Microsoft Excel spreadsheet and PDF files.

   PROS: Cheapest option

   CONS: Not as convenient

PRODUCTION

After review is complete, the next stage is Production. Regardless of your review method, you want to do what you've always done: Pull out the responsive documents and confirm you didn't accidentally sweep in anything privileged. How you go about doing this will vary greatly based on whether or not you used review software. Even if you used review software, the processes for generating productions are all different. So instead of focusing on how to isolate your production set, we're going to focus on what you're going to give to opposing counsel and what you can expect to receive from opposing counsel.

The most important thing to remember about production is "what is good for the goose is good for the gander." You should produce documents in a similar manner that your receive them. If production methods have not yet been discussed (for example, at a Rule 26(f) or Case Management conference), it's not too late. Before you send anything out you can still check with the other side to see what they plan on producing. Because you want to exchange the same things. If opposing counsel is not going to give you metadata, you don't want to give them metadata. And so forth.

There are many different methods or production and the E-Discovery reference model discusses standards for each of them. Productions generally come in the following format (or some combination thereof):

PAPER - Please don't produce e-discovery in paper! This helps no one and it's expensive.

PDF – If you'll be producing in PDF format, you'll need to decide whether you're providing single or multipage PDFs and whether or not they're text searchable.

OCR (Optical character recognition) - These files make documents text searchable. If you are using review software, you may already have OCR text files. Confirm that vendors and software programs will take your redactions into account. You don't want to redact a sentence out of the image, only to provide that same text in an OCR file.

Single image tiffs with a load file (with or without OCR). These files will enable the recipient to load the documents into e-discovery software. Single image tiffs are image files, one document per page. The Load file tells the software where each document starts and ends and also identifies the metadata associated with each document. Load files can come in specialty formats (DII, DAT, OPT) or TXT or

PRACTICE TIP

BEST FORMATS FOR PRODUCTION OF E-DISCOVERY DOCUMENTS

PDF. Options include single or multi-page PDFs and whether or not they are text searchable.

OCR. (Optical Character Recognition) Text-searchable documents.

SINGLE IMAGE TIFFS. Allows recipient to load the documents into e-discovery software.

CSV format. You should be able to open all these (except for CSV) using NotePad. A CSV file (comma separated value) can be opened using Excel. Beware that load files can be difficult to interpret before you get the hang of it. Ask your vendor to help you decode them.

Natives – it is pretty common to exchange native excels and other multimedia files. The documents should be renamed with the Bates Number.

If you don't have document review software and you receive a production that is in Tiff/Load File Format with OCR, be aware that they contain a lot of usable information! You can ask a vendor to convert that load file to excel format, and ask them to convert those tiffs to multipage PDFs. Then you can review other parties' productions in the same manner that we discussed above. Navigate through an excel file, and open PDFs as you go along.

> **Before you send anything out you can still check with the other side to see what they plan on producing. Because you want to exchange the same things. If opposing counsel is not going to give you metadata, you don't want to give them metadata.**

CONCLUSION

The goal of this practice guide was to de-mystify the process of e-Discovery by providing a basic overview. As you execute your e-discovery plan, you will likely develop your own methods and preferences. While the EDRM does provide guidelines and standards, there are many ways of doing things. Good luck!

LITIGATION HOLD NOTICE - PLAINTIFF

To: **[KEY CUSTODIANS]**

From: **[LEGAL/OFFICER]**

Date:

Re: Litigation Hold Notice – Effective Immediately
[CASE NAME]

[CLIENT] has recently filed a civil lawsuit against **[DEFENDANT]** in the **[COURT]**. We have retained counsel to prosecute the case and are being represented by **[ATTORNEY(S)]**, who can be contacted at **[CONTACT INFO]**.

[CLIENT] asserts **[GENERAL DESCRIPTION]**. Specifically, **[DESCRIBE EACH COUNT]**. We have a legal duty to preserve all documents (paper and electronically stored information, or ESI) and other evidence that are, or may be, relevant to this dispute. For this reason, it is essential that you **IMMEDIATELY** preserve and retain all potentially relevant evidence.

You are receiving this Notice because we believe you may have potentially relevant evidence. The purpose of this Notice is to instruct you on the preservation process. These instructions supersede any other record retention policy. The relevant documents **MUST** be preserved, even if **[CLIENT]**'s record-keeping guidelines (formal or informal) otherwise would allow you to delete or otherwise destroy material.

General Instructions re: Preservation

Preservation should be interpreted broadly to accomplish the goal of identifying all potentially relevant documents, maintaining the integrity of the documents as they currently exist and **ensuring that they are not altered, deleted, destroyed or otherwise modified**. If you have any doubt as to whether a document or category of documents is covered by this Notice, please err on the side of preservation. Among other things, saving these documents will assist **[CLIENT]** in its prosecution of this case against **[DEFENDANT]**. Your obligation to preserve extends to all potentially relevant documents in your possession, custody or control. Examples of documents that are not in your possession or custody, but remain subject to your control, include documents in the possession or custody of employees who report to you, or documents in the possession or custody of third parties such as contractors or advisers hired to do work for **[CLIENT]**.

At this time, this Notice requires only that you **PRESERVE** potentially relevant documents. You should **NOT** copy, move, forward or otherwise collect potentially relevant documents unless directed to do so by our attorneys. This is especially critical for ESI, as there is electronic information called "metadata" that does not appear on the printed version of an electronic document, but provides critical information about the data and must be preserved, along with any directory and/or folder information about where the data is stored.

What to Preserve

Until further written notice from counsel or from me, you must not alter, delete, destroy or otherwise modify potentially relevant documents. Please note that you must preserve all non-identical copies of potentially relevant documents, so if one copy contains handwritten notes and the other does not, both should be preserved. Similarly, drafts of potentially relevant documents, to the extent they exist, should be preserved. Unless otherwise stated, the relevant time period begins on [DATE], and continues into the future.

Potentially relevant documents include but are not limited to the following categories:

* [INSERT SPECIFIC CATEGORIES]

Where Are the Documents Located?

While it generally is easy to locate and preserve potentially relevant paper records, potentially relevant electronically stored information may exist in many different forms and be found in a variety of locations. The following, while not exhaustive, should be considered as sources of potentially relevant ESI:

1. Email messages and their attachments, including messages in your "Inbox," "Sent Items," and "Deleted Items" folders, in any personal folders, "archives" or PSTs you have created, and in any other email accounts you may use, including personal accounts (e.g., Gmail, Yahoo, Facebook, etc);

2. Word processing documents, spreadsheets, analyses and presentations, including items stored in your "My Documents" folder, in shared folders, on network drives, on the home drive of your company desktop/laptop, or on your personal or home computer;

3. Any of the above stored in common locations (such as Intranet or SharePoint sites); on portable electronic devices (such as a BlackBerry or other SmartPhone or cell phone); or on external storage devices (such as CDs, DVDs, external hard drives, flash drives);

[ONLY INCLUDE FOLLOWING IF CASE WARRANTS]

4. Electronic calendars, diaries, notes and/or tasks;

5. Databases;

6. Websites/Social Media sites;

7. Voicemail;

8. Legacy Equipment (equipment [CLIENT] no longer uses in the normal course of business); and

9. Former Employees' Computers: Take any necessary steps to preserve information from computers or other devices with potentially relevant information of former employees or other equipment no longer in use but still within [CLIENT]'s possession or control.

Please note that these lists are not all-inclusive, but simply represent our best assessment at this time of (i) what categories of information might be relevant and (2) where documents might be located. Please interpret these lists broadly and err on the side of preservation.

We will continue to work with our attorneys and our IT staff to determine the most reasonable and least disruptive way to identify and preserve potentially relevant documents. I will contact you if any additional steps should be taken to review, segregate, or collect any paper documents or ESI. For now, there is no need for you to take any steps OTHER THAN continuing to make sure you do not alter, delete, destroy or otherwise modify potentially relevant documents.

[CLIENT] takes its preservation obligations very seriously. The procedures described in this Notice override any routine retention or destruction policies that you currently follow. If you have any questions regarding any aspect of the Notice or the preservation process, please err on the side of caution and contact counsel or me. Thank you for your cooperation with respect to this important matter.

ACKNOWLEDGMENT

I have reviewed the above Notice and agree to follow the preservation instructions in that Notice.

Signature: _____

Name (printed): _____

Date: _____

PLEASE RETURN THIS SIGNED DOCUMENT TO [SENDER] BY [DATE]

DISTRIBUTION LIST

[INSERT KEY CUSTODIANS]

[INSERT IT REPRESENTATIVE]

[INSERT HR REPRESENTATIVE]

LITIGATION HOLD NOTICE - DEFENDANT

To: [KEY CUSTODIANS]

From: [LEGAL/OFFICER]

Date:

Re: Litigation Hold Notice – Effective Immediately
[CASE NAME]

[**CLIENT**] has been named a defendant in a civil lawsuit filed by [**OPPOSING PARTY**] in the [**COURT**]. We have retained counsel to defend the case and are being represented by [**ATTORNEY(S)**], who can be contacted at [**CONTACT INFO**].

The Plaintiff alleges [**GENERAL DESCRIPTION**]. Specifically, the Plaintiff claims [**SPECIFIC DESCRIPTION OF EACH COUNT**]. We have a legal duty to preserve all documents (paper and electronically stored information, or ESI) and other evidence that are, or may be, relevant to this dispute. For this reason, it is essential that you IMMEDIATELY preserve and retain all potentially relevant evidence.

You are receiving this Notice because we believe you may have potentially relevant evidence. The purpose of this Notice is to instruct you on the preservation process. *These instructions supersede any other record retention policy. The relevant documents MUST be preserved, even if [**CLIENT**]'s record-keeping guidelines (formal or informal) otherwise would allow you to delete or otherwise destroy material.*

General Instructions re: Preservation

Preservation should be interpreted broadly to accomplish the goal of identifying all potentially relevant documents, maintaining the integrity of the documents as they currently exist and **ensuring that they are not altered, deleted, destroyed or otherwise modified**. If you have any doubt as to whether a document or category of documents is covered by this Notice, please err on the side of preservation. Among other things, saving these documents will assist [**CLIENT**] in its defense against the Plaintiff's claims. Your obligation to preserve extends to all potentially relevant documents in your possession, custody or control. Examples of documents that are not in your possession or custody, but remain subject to your control, include documents in the possession or custody of employees who report to you, or documents in the possession or custody of third parties such as contractors or advisers hired to do work for [**CLIENT**].

At this time, this Notice requires only that you **PRESERVE** potentially relevant documents. You should NOT copy, move, forward or otherwise collect potentially relevant documents unless directed to do so by our attorneys. This is especially critical for ESI, as there is electronic information called "metadata" that does not appear on the printed version of an electronic document, but provides critical information about the data and must be preserved, along with any directory and/or folder information about where the data is stored.

What to Preserve

Until further written notice from counsel or from me, you must not alter, delete, destroy or otherwise modify potentially relevant documents. Please note that you must preserve all non-identical copies of potentially relevant

documents, so if one copy contains handwritten notes and the other does not, both should be preserved. Similarly, drafts of potentially relevant documents, to the extent they exist, should be preserved. **Unless otherwise stated, the relevant time period begins on [DATE], and continues into the future.**

Potentially relevant documents include but are not limited to the following categories:

* [**INSERT SPECIFIC CATEGORIES**]

Where Are the Documents Located?

While it generally is easy to locate and preserve potentially relevant paper records, potentially relevant electronically stored information may exist in many different forms and be found in a variety of locations. The following, while not exhaustive, should be considered as sources of potentially relevant ESI:

1. Email messages and their attachments, including messages in your "Inbox," "Sent Items," and "Deleted Items" folders, in any personal folders, "archives" or PSTs you have created, and in any other email accounts you may use, including personal accounts (*e.g.*, Gmail, Yahoo, Facebook, etc);

2. Word processing documents, spreadsheets, analyses and presentations, including items stored in your "My Documents" folder, in shared folders, on network drives, on the home drive of your company desktop/laptop, or on your personal or home computer;

3. Any of the above stored in common locations (such as Intranet or SharePoint sites); on portable electronic devices (such as a BlackBerry or other SmartPhone or cell phone); or on external storage devices (such as CDs, DVDs, external hard drives, flash drives);

[**ONLY INCLUDE FOLLOWING IF CASE WARRANTS**]

4. Electronic calendars, diaries, notes and/or tasks;

5. Databases;

6. Websites/Social Media sites;

7. Voicemail;

8. Legacy Equipment (equipment [**CLIENT**] no longer uses in the normal course of business); and

9. Former Employees' Computers: Take any necessary steps to preserve information from computers or other devices with potentially relevant information of former employees or other equipment no longer in use but still within [**CLIENT**]'s possession or control.

Please note that these lists are not all-inclusive, but simply represent our best assessment at this time of (i) what categories of information might be relevant and (2) where documents might be located. Please interpret these lists broadly and err on the side of preservation.

We will continue to work with our attorneys and our IT staff to determine the most reasonable and least disruptive way to identify and preserve potentially relevant documents. I will contact you if any additional steps should be taken to review, segregate, or collect any paper documents or ESI. **For now, there is no need for you to take any steps OTHER THAN continuing to make sure you do not alter, delete, destroy or otherwise modify potentially relevant documents.**

[**CLIENT**] takes its preservation obligations very seriously. **The procedures described in this Notice override any routine retention or destruction policies that you currently follow. If you have any questions regarding any aspect of the Notice or the preservation process, please err on the side of caution and contact counsel or me.** Thank you for your cooperation with respect to this important matter.

ACKNOWLEDGMENT

I have reviewed the above Notice and agree to follow the preservation instructions in that Notice.

Signature: _____

Name (printed): _____

Date: _____

PLEASE RETURN THIS SIGNED DOCUMENT TO [SENDER] BY [DATE]

DISTRIBUTION LIST

[INSERT KEY CUSTODIANS]

[INSERT IT REPRESENTATIVE]

[INSERT HR REPRESENTATIVE]

PRESERVATION NOTICE - THIRD PARTY

[DATE]

[NAME]
[ADDRESS]

Re: Preservation Notice – Effective Immediately

Dear **[NAME]:**

I am writing to you on behalf of my client, **[CLIENT**]. As you may know, [CLIENT] is engaged in a lawsuit with [OPPONENT] regarding **[BRIEF DESCRIPTION OF LAWSUIT]**. As a party to this suit, **[CLIENT]** is obligated to take steps to preserve all potentially relevant evidence. This can include evidence in the possession, custody or control of third parties like **[RECIPIENT]**.

Accordingly, please take all necessary steps to preserve any documents or electronically stored information (ESI) that could be considered relevant to this dispute. All emails and ESI should be preserved in electronic form. Specifically, please preserve **[DESCRIPTION]**. To the extent that you have any other emails, ESI or documents that may be relevant, please preserve those as well. I will follow up with you as the case progresses to determine how best to retrieve what you are preserving.

I appreciate your prompt attention to this matter. Please do not hesitate to contact me if you have any questions.

Sincerely,

[COUNSEL]