LITIGATION HOLD NOTICE

Post-Filing of Litigation

Attorney-Client Privileged Communication

[Memo addressed to a targeted, limited group of individuals reasonably likely to have responsive documents]:

As a result of a lawsuit that has been filed against [Entity], it is imperative that [Agency] preserve all documents and electronic information that may be relevant to the claims in the case. This memorandum is being addressed to you because you have been identified as an individual who may have documents and electronic information that are related to these claims.

You are directed not to discuss the claims at issue, or the contents of this memorandum, without first discussing them with legal counsel. Legal counsel can assist you with your duties to comply with the terms of this memorandum. This direction is made to ensure that the rights and interests of all individuals involved with these claims, including the right of privacy, are safeguarded. It is also made to ensure that attorney-client privileges are preserved.

The claims in the lawsuit are as follows: [define]

Because many of the claims in the lawsuit are general, it is difficult at this time to narrow the scope of what categories and types of documents and electronic information must be retained. You should, therefore, err on the side of preservation. Further, you must undertake retention of this information regardless of [Entity] retention policies or any other policies applicable to the documents. You should also note that electronic information includes emails, voicemail messages, and all types of information that is commonly created, stored, and transferred by computer.

_____ Is assigned to handle this litigation and will be in contact with you shortly to provide you with further guidance and discuss any questions you may have. In the meantime, do not hesitate to contact _____ or _____.

LITIGATION HOLD NOTICE

To: Employees of _____

From: _____

Date: _____

Re: Litigation Hold Notice – Effective Immediately

_____ has recently filed a civil lawsuit against _____. in the _____, Court of Florida. We have retained counsel to prosecute the case and are being represented by _____, who can be contacted at: _____

_____has 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. This notice does not mean that you are necessarily involved in the dispute; however, _____ is under a legal duty to preserve all evidence, whether printed or electronic form, that might become relevant to this matter (and to continue to preserve such evidence related to the matter). Some of this information may be in your possession or control, and as an employee, you have a legal duty to preserve that information, even if in the normal course of operations those records could be deleted; to satisfy our legal obligations, we require your assistance in preserving documents and electronic data. 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 _____ 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 _____ in its prosecution of this action. 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 _____.

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 _____, and continues into the future.**

The following information might be relevant to the dispute: Personnel files, Emails, Meeting notes, Investigation reports, etc. In identifying and preserving the above documents and data, please keep in mind that documents and electronic data include, but are not limited to, application files, drafts, correspondence, telephone logs, e-mail, text files (including word processing documents and presentations), journal or calendar entries, calendar and scheduling information, task lists, notes, Blackberry messages, voice-mails, spreadsheets, reports, invoices, purchases orders, meeting minutes, working files, databases containing information, computer system activity logs, internet usage files, and network access information.

Where Are the Documents Located?

While it is generally 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 you "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, Iphone, or other SmartPhone or cell phone); or on external storage devices (such as CDs, DVDs, external hard drives, thumb drives, flash drives);

4. Electronic calendars;

5. Databases;

6. Voicemail;

7. 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 _____ 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 ii) where documents might be located. Please interpret these lists broadly and err on the side of preservation.

Things to do Now

You are required to take the following steps immediately to protect and preserve any of the information that is in your possession or under your control until further notice. Specifically:

1. Suspend deletion, overwriting, or any other destruction of electronic information relevant to this dispute. This includes electronic information wherever it is stored – at your workstation, on a laptop, on your cell phone, on an external storage device, such as a thumb-drive, or at home. This includes all forms of electronic communication (e.g. email, word processing, calendars, voice messages, videos, photographs, information on your cell phone or PDA). The information must be preserved in its original electronic form, so that all information contained within it, whether visible or not, is also available for inspection – i.e., it is not sufficient to make a hard copy of electronic communication.
2. For electronic materials, you should create an electronic folder and move all e-mails, word documents, pdfs, other electronically stored data, etc. into that folder. For hard-copy materials, notes, etc., you should put them in a folder in a secure space.
3. Similarly, preserve any new electronic information that is generated after you receive this notice that could be considered relevant to this dispute.
4. Preserve any hard copy under your control.
5. At the network and systems administration level, this directive requires you to preserve and retain all potentially relevant files stored on the servers and to refrain from doing any administrative work that has the potential to destroy potentially relevant files. Any "janitorial" functions must be disabled. All backup tapes must be preserved and pulled from recycling rotation for any materials in existence.

This is an important legal duty and failure to follow these instructions may subject you to discipline, as the failure to preserve this information has very serious consequences for the agency.

We will continue to work with our attorneys and our IT staff to determine the most reasonable and least disruptive ways 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 <u>other than</u> continuing to make sure that you do no alter, delete, destroy or otherwise modify potentially relevant documents.**

_____ takes its preservation obligations very seriously. **The procedures described in this Notice override any routine retention or destruction policies that you currently follow.**

Please execute and return to _____, as _____, as soon as possible the attached CERTIFICATION OF RECEIPT AND COMPLIANCE WITH LEGAL HOLD MEMORANDUM, confirming that you have received, read, understand and intend to comply with this directive. This is an important legal duty and failure to follow these instructions may subject you to discipline, as the failure to preserve information has very serious consequences for _____.

Please advise us immediately if you have any questions about, or any problems complying with this Legal Hold Memorandum. Please notify us if you are aware of individuals (other than those listed above) or third parties who may have documentation/information and or should receive this Legal Hold Memorandum.

Thank you for your cooperation with respect to this important matter.

CERTIFICATION OF RECEIPT AND COMPLIANCE WITH
LEGAL HOLD MEMORANDUM

I hereby certify that I have received a copy of the LEGAL HOLD MEMORANDUM dated _____, and that I have read and understand the same. I certify that I will comply with the requirements of the LEGAL HOLD MEMORANDUM. I further certify that I will advise _____, as _____, if I have any questions regarding my duties and responsibilities under the LEGAL HOLD MEMORANDUM or if I become aware of any instances in which I or anyone else fails to comply with the LEGAL HOLD MEMORANDUM.

Signed: _____

Printed Name: _____

Dated: _____

LITIGATION HOLD NOTICE

DATE: _____

TO: CLIENT REPRSENTATIVE/PRESIDENT-OWNER
(DECISION MAKER)

Re: _____
E-discovery issues ("ESI")

Dear_____:

The below summary and proposed discovery plan is tendered to you so that you are aware of the expectations as it relates to electronic discovery, which also identifies certain minimum steps that the court will expect us to undertake, particularly as it pertains to electronically stored information ("ESI").

As in many lawsuits, Requests for Production as served that are very broad and expansive, which are tailored to cover erased but retrievable information, native format delivery. This vast request is typical of a party who either seeks to harass, or who is not familiar with requests for ESI, or who simply wants to set opposing parties up for a future motion for sanctions for failure to preserve or produce the ESI.

As you may or may not know, the law applicable to ESI discovery is rapidly changing. Not only must a party produce materials that are obviously relevant and responsive but it must be sure to use the *best practices* in that production, including both hard version and ESI documents, and that it satisfies any new requirements as they evolve. The Florida Rules of Civil Procedure are currently being amended to include some parameters for the appropriate protocols for ESI discovery issues by developing specific procedures particular to ESI. As it currently stands, the courts have little express guidance form the Rules or case law. The handful of cases that have been reported make it clear that without collaboration, a well thought eDiscovery response plan, and some sense of urgency, this whole eDiscovery process can become rife with mistakes that may result in some pretty unpleasant and expensive consequences. It almost goes without saying that this is an area that is ripe for mischief and we clearly have some lawyers involved in this case who are prone to dissembling and even cheating if they think they can get away with it. The last thing that we want to do is "litigate the litigation" through real and imagined discovery disputes.

This type of production will be very expensive for both sides; to obtain all of this information, then to sort through it and cull the responsive documents while in these formats, then to review everything and finally produce it. Most of the information will be gibberish to an attorney. Frankly, forensic experts would probably be necessary for either side to make any use of it. We doubt that this is what any party really wants and we certainly would much prefer to avoid having to go to the lengths required to produce the data in the formats requested, but there are duties of the parties that cannot go unanswered. Furthermore, much of the information will be subject to one or more privileges or will otherwise be protected. Therefore, we suggest the following strategy.

Here are some of the preliminary steps we need to complete before starting the process of collecting, culling and eventually producing documents:

The first step is the simplest and least expensive. Since we are required to "preserve" all of the ESI information and do not know what that might cover at this stage, the most practical tactic is to make one copy of all of the accessible information at one time and store it in a safe and secure manner. The nature of ESI makes it ephemeral; especially the locations, the metadata and all of the other unseen information. The metadata (including the "to, from, time sent, and subject lines of an email") can prove very useful during eDiscovery as these files can make it clear who knew what and when they knew it.

A practical alternative is to obtain a forensic image of each PC, server, or other electronic storage media. This process results in an exact replica of that media and gives a more complete picture than just what can be burned to a DVD or put on an external hard drive. To the extent there are any, you should also include electronic faxes, voicemails, digital audio and video recordings, and other potential sources of information, such as instant messaging archives, or cellphone logs. These data sources may contain not only actual information, but (in some cases) also metadata. To be clear, I doubt that even a small percentage of this information would be responsive and a very small percentage would actually be produced in any format. This step is merely a precaution so that we can tell the court, in complete candor, that _____ has properly preserved any possible ESI for future analysis and no one can ever claim that anything was lost or concealed. Fortunately, this critical step of preservation does not have to be expensive or time consuming.

It is essential to capture the entire media with the full spectrum of the data so that no matter how the case dynamics might change the data will still be available for analysis. At this point we will need to determine if there are "gaps" in the data – i.e., has any data been lost or destroyed. This would be the time to determine whether this was due to routine operation of the computer systems so we can explain and defend such gaps at the meet and confer sessions with opposing counsel. Thus, we should discuss this initial step in the immediate near future.

Once the data preservation step has been completed, we need to identify the people, places, and events that are important to the case. We need to identify the person(s) who have firsthand working knowledge of _____ records and databases. We will need to know others' expertise areas and their general technical qualifications. Specifically, we will need to know your employee's understanding of the maintenance and operation of _____databases and their experience in responding to document requests whether in the context of litigation, audits, etc.

Whoever serves as the client's e-discovery liaison will need to provide us with the following information:

a. The location and approximate size of all databases that may contain potentially responsive documents;
b. The nature of the documents that are maintained by _____ in the databases – i.e. what sort of records are kept in each database;
c. The retention policy of _____. If ESI is purged or deleted from the databases, is this pursuant to a formal policy? If there is no formal policy, we will need to speak with someone who can identify the reasons behind the deletion of information;
d. Determine what is accessible and inaccessible data (based on undue burden and cost, this will be the basis of any cost-shifting request);
e. Who are the potentially relevant custodians;
f. Discuss potential critical key words (i.e., the language _____ uses to discuss these issues and people).

Next, we will get together with you and the in-house eDiscovery liaison and discuss the following:

a. Determine the size, scope and timeframe of collection;
b. Determine the best method of collection – whether it will be in-house or through a third-party vendor;
c. An estimate of the time required to conduct a search of the databases to identify potentially responsive documents;
d. Discuss a discovery budget;
e. Formulate a cost-effective yet fair scope of discovery to be presented to opposing counsel, including:

    i. The number of relevant custodians
    ii. File types and locations
    iii. Accessible vs. inaccessible ESI
    iv. The format of production
    v. A reasonable timeframe
    vi. The potential for cost shifting

f. Discuss the nature and extent of applicable privileges that restrict the disclosure of documents;
g. Discuss the method and procedure of identifying these privileged documents and a cost estimate for such;
h. Determine whether we request cost-shifting and consider how to best defend a cost-shifting request from opposing counsel. We will discuss how to maximize cost-shifting opportunities keeping in mind this 2-step test: (1) the responding party must demonstrate that the information sought is "not reasonably accessible because of undue burden or cost" and (2) once this showing is made, the burden of proof shifts to the requesting party, who must show that there is "good cause" for requesting the information;
i. Come up with concrete search terms or words to present to opposing counsel.

The ordinary and predictable costs of discovery are usually borne by the producing party. However, the courts may shift costs where the demand is unduly burdensome because of the nature of the effort involved to comply. Traditionally, the consideration of cost-shifting by the courts has been at the discretion of the court. The Federal Rules concerning eDiscovery specifically note that an order compelling the production of ESI that is "not reasonably accessible" may be subject to conditions, including "payment by the requesting party of part or all of the reasonable costs of obtaining information from sources that are not reasonably accessible." *See* FRCP 26(b)(2)(B). That Rule then identifies seven factors to be considered, and it is likely that our state courts addressing production under those rules will routinely consider, if not order, cost-shifting or cost sharing. The types of information that typically may (but not always) fall within the "not reasonably accessible" category include deleted data, disaster recovery/backup tapes, residual data, and legacy data.

It should also be remembered that even though the ESI is reasonably accessible (e.g., it exists on a corporate storage area network), cost-sharing and cost-shifting may still be available if the aggregate volume of data requested is disproportionate to the needs in the case and/or the respective resources of the parties such that a condition of further discovery can be the shifting of some or all costs of such discovery.

The factors for cost-shifting for the production of "burdensome electronically stored information" (whether reasonably available or accessible or not) should include (in order of importance):

- Whether the information is reasonably accessible as a technical matter, without undue burden or cost;
- The extent to which the request is specifically tailored to discovery of relevant information;
- The availability of such information from other sources, including testimony, requests for admission, interrogatories, and other discovery responses;
- The total cost of production, compared to the amount in controversy;
- The total cost of production, compared to the resources available to each party;
- The relative ability of each party to control costs and its incentive to do so;
- The importance of the issues at stake in the litigation; and,
- The relative benefits to the parties of obtaining the information.

Finally, consideration of the "total cost of production" includes the estimated costs of reviewing retrieved documents for privilege, confidentiality, and privacy purposes. It also includes consideration of opportunity costs or disruption to the organization, e.g., the need to redirect IT staff from business projects to retrieve or review the data. Another thing to keep in mind is that conducting eDiscovery in-house can lead to difficulties in separating costs used in eDiscovery from day-to-day operation costs. We will need to make sure that we track all expenses carefully and should consider using a service provider that delivers a clean, itemized bill. These steps can help us garner a better understanding of what the process costs and also make it easier to negotiate who's paying for what.

Thereafter we will need to prepare the data for analysis (this is often referred to as early case assessment - "ECA") and this needs to be done before we meet with opposing counsel. ECA is the practice of culling down the collection of unstructured documents – often by completely removing 50% or more of the documents – prior to going into active document searching and review. This is often done by using metadata (such as date or author), keywords or concepts, and removing documents that contain certain obviously non-relevant terms.

In order to perform an ECA, the data must be put in an appropriate form for subsequent analysis, which can involve several steps. It can require imaging the original media so that it is in both a protected and analyzable form. It can also employ various processes that make the most of the data, including confirming file signatures, recovering deleted files and folders using both the file system and data carving techniques, and indexing the data in preparation for word searching. Vendors provide software to assist with this preparation.

Some primary goals of this initial data processing are to discern at document or item-level exactly what data is contained in the universe collected; to record all item-level metadata as it existed prior to processing; and to enable defensible reduction of data by "selecting" only appropriate items to move forward to review. This phase of the process requires strict adherence to process auditing, quality control, analysis and validation, and attention to chain of custody considerations.

In many cases, electronically stored information is found in broad groupings based on the "container" and not the "content," such as an email "inbox" or "outbox," or on a shared drive, or on a web server. In many instances, such unstructured or semi-structured data is not archived in a manner that can be used to readily identify relevant information. Data may arrive at the processing stage in various formats which then need to be restored before subsequent work can be done (tapes, backups, etc.);

individual files and emails may need to be extracted from container files (PST, NSF, zip, rar, etc.); and certain types of data may need to be converted to facilitate further processing (legacy mail formats; legacy file formats). During these processing stages individual items are cataloged and their associated metadata is captured.

It is hardly ever necessary to review all of the items that are submitted for analysis, and in light of the nature of the requests made here it unlikely that more than a very small number of documents will require a review. A number of data reduction opportunities are usually available. Processing is further broken into four main sub-processes, namely: Assessment; Preparation; Selection; and Output. Assessment may allow for a determination that certain data need not move forward; Preparation involves performing activities against the data which will later allow for specific item-level selection to occur (extraction, indexing, hashing, etc.); Selection involves de-duplication; searching; and analytical methods for choosing specific items which will be moved forward.

Indexing is the universal term for coding and data entry. The index is a searchable catalog of documents created by search engine software whereby database fields are used to categorize and organize documents. Indexing is particularly important because no matter how diligently you search, you can't find something if it isn't there. Such is the case with document text. If the text is not indexed, your search will not find it. Search engines don't actually search the text of the documents. Rather, they search an index of the text of the documents. If the document contains no readable text to be indexed, or if the document is not properly indexed, the document will not be found. The danger, of course, is that the searcher may believe the search was complete when, in fact, it was not. The search may have found all matching text, but it may have overlooked matching documents whose text was not readable.

There are several reasons why a document's text may not be indexed:

- No text due to file type. Typically, text can be extracted only from standard applications. The document may have been created in an application from which text cannot easily be extracted, or it may be a photo or other file that has no text.

- No OCR (or bad OCR). A file that is scanned into TIFF without text or PDF (image only) format requires OCR software to create the indexable text. If the file is not run through OCR or if the OCR program or process is deficient, the text will exist in a way that it cannot be indexed.

- Hardware or software error. As with any computer application, sometimes there can be "hiccups" in the indexing process, requiring that the documents be re-indexed. To avoid this situation, quality control following indexing is essential.

- Human error. A technician can make mistakes that prevent proper indexing, such as incorrect mapping to the text in the load file or incorrect copying of the data so that the mapping is incorrect. Again, quality control should uncover these errors.

- Password protection. Indexing will skip password-protected documents. You need to identify them and either get the password or break the password (if possible).

- Office 2007/2010. When Microsoft first released Office 2007 and its new document format, many systems were unable to read it. By now, most systems have caught up and

have the ability to extract text from Office 2007/2010 files. However, a document collection may include Office 2007 documents that contain non-indexable text (or text that hasn't been indexed).

Beware of the old proverb, "What you don't know can't hurt you" because that is certainly not the case in eDiscovery. One danger when the search index omits document text is that counsel will fail to produce a responsive document. If this happens by a good faith mistake, it is unlikely to result in sanctions. For one, the other side is unlikely to know about the omission. For another, the attorneys for the producing party may not even know about it.

The greater danger in this scenario is that counsel will inadvertently produce a privileged document–and that IS a big problem. That was part of what lead to the disastrous outcome in *Mt. Hawley Insurance Company v. Felman Production Inc.*, 2010 WL 1990555 (S.D.W.Va., May 18, 2010), a case in which counsel inadvertently produced a "smoking gun" document. (Even if the court enforced the clawback agreement, turning over the smoking gun documents that didn't hit on the privilege search would still have been a disaster. This bell could not be unrung.)

While non-indexed documents pose dangers, they are dangers that we can minimize or avoid altogether by implementing these best practices:

- After the data is loaded, get an exception report that show non-indexed data by file type, and look carefully at the counts.
- Sample the non-indexed data by file type. Does any of the data need OCR?
- When you run searches, be sure to sample the non-hits as well as the hits.
- Remember to do sweep searches later to look for any documents that become searchable but that were not searchable when searches were previously run.

The actual production can be a "peel the onion" kind of approach. The first step can be the production of lists that disclose the names of files contained in the filing system. Although lists are sometimes not informative enough, they, nonetheless, are a good first step that allows the requesting party to see what is available and how their requests can be better targeted. In addition, these lists provide useful attribute information that confirm or deny attempted spoliation as well as provide important usage and trend information about the media and the data it contains. It is often helpful to have this list before the initial meeting with opposing counsel as a show of good faith.

We must emphasize that *all* of the foregoing is a prelude to the "meet and confer" with opposing counsel and we must be in possession of specifics by the time we have that meeting. When we take that next step and meet with opposing counsel we will try to come to an agreement concerning the scope of discovery and other critical factors, and to either develop an agreed plan with counsel or seek the court's assistance in ordering one so that we have rules in place before we ever start to gather the information to produce. Reasonableness and proportionality will be key issues here. Some of the things that must be discussed include the production of inaccessible data, how the parties will handle duplicates, keyword search terms, the form of production, a Bates scheme, cost-shifting negotiations, and how we want to handle confidential, trade secret, and business sensitive data. It is at this meeting that we will produce the lists complied that disclose the names of files contained in the filing system as a show of good faith and we will use this list to negotiate the scope of discovery. One of the most important aspects of this meeting with opposing counsel is the "clawback provision." A clawback provision provides that the disclosure of attorney-client or work product information does not waive either privilege, so long as (1) the disclosure was inadvertent, (2) the holder of the privilege took reasonable steps to prevent the disclosure, and (3) the holder promptly took reasonable steps to rectify the error.

After meeting with opposing counsel, we will start the process of culling through the information. This is where we will need to decide if we will be handling this in-house or if we will be using a third party vendor, which I discuss below. In order to keep costs low, for both the technical experts and the legal staff, it is important to streamline the population. Streamlining the population can involve many steps such as removing duplicates and removing known files like operating systems and application program files, from consideration. Once the population is properly prepared, the next step is to start sifting through the data. Searches can be term searches, context searches or even network searches. Each has its advantages and disadvantages. Like other parts of this process, searching can be an iterative process. As results are learned, refinements can be made to more accurately identify the desired target.

After identifying the desired targets, excluding privilege items is the next step. The same search techniques can be used but their populations narrowed to the responsive targets. At that stage, if any information is highly confidential or otherwise protected, we will identify those issues, try to resolve them or have the court resolve any dispute before we produce the data.

Before assuming that the search is complete, we will validate the population. This can be done by examining metadata contained in various artifacts and system resources. The objective is to confirm that all of the relevant media has been preserved and subjected to search. And then, of course, the final step is to produce the data.

As to the pros and cons of performing these steps in-house vs. hiring a third party vendor, in most cases, letting someone outside of the corporation handle eDiscovery is a good idea. Litigation support vendors help with data deduplication, culling, processing, and analyzing the information before the contract document reviewers see the documents. You manage costs by managing risk and its attendant expenses. When a third-party handles the collection and processing, it can benefit the investigation in two ways: (1) a service provider expert, not a corporate employee, testifies in this case; and (2) an expert can explain any anomalies in the data with more credibility than someone involved in the process.

While litigation has long been a fact of life for business, eDiscovery issues have come to the forefront only in the past few years. A resource, often considered as an in-house source of eDiscovery expertise, is one or more non-attorney employees of the firm or company whose sole responsibility is to understand and manage the technical side of litigation support involving eDiscovery. The benefits of having your own in-house eDiscovery expertise seem obvious – ease of access, ease of supervision, ability to work with known and trusted personnel, common goals, etc. The effort to develop and maintain the now-considerable level of expertise needed to understand and manage the technical aspects of eDiscovery in-house may be possible (and seem an attractive way to save costs), but it presents a number of risks.

First, there is a non-productive use of employee or attorney time to obtain and maintain the necessary knowledge and expertise to be able to understand and manage eDiscovery technology. The more time an attorney is busy with litigation, the less time that attorney has available to devote to the study necessary to stay current with eDiscovery technology and practice (and vice versa).

Second, an attorney incurs the additional risk of professional sanctions based upon any violation of the ethical rules that govern his or her work as an eDiscovery expert:

Responsibilities Regarding Law-Related Services (a) A lawyer shall be subject to the Rules of Professional Conduct with respect to the provision of law-related services, as defined in paragraph (b), if

the law-related services are provided: (1) by the lawyer in circumstances that are not distinct from the lawyer's provision of legal services to clients; or (2) in other circumstances by an entity controlled by the lawyer individually or with others if the lawyer fails to take reasonable measures to assure that a person obtaining the law-related services knows that the services are not legal services and that the protections of the client-lawyer relationship do not exist. (b) The term "law-related services" denotes services that might reasonably be performed in conjunction with and in substance are related to the provision of legal services, and that are not prohibited as unauthorized practice of law when provided by a non-lawyer.

Another important cost that must be weighed when considering the use of in-house expertise for eDiscovery compliance is the attendant liability for one's own failures, whether or not those failures were unintentional, negligent, or unforeseeable. If your company or firm takes on the burden of handling eDiscovery compliance, it also takes on the liability for ALL mistakes, tardiness and failures to comply with discovery rules and court orders.

Most executives are not experts in the technology, protocols and techniques now required by the courts in responding to discovery orders involving ESI. Failures, negligent mistakes or intentional misconduct in responding to eDiscovery obligations have resulted in sanctions that range from embarrassing comments in published opinions ("Any competent electronic discovery effort would have located this email." *Green v. Blitz U.S.A., Inc.*, No. 2:07-CV-372, 2011 U.S. Dist. LEXIS 20353 (E.D. Tex., Mar. 1, 2011)) to possible imprisonment for contempt of court, the imposition of a default judgment for the opposing party, and the award of attorney's fees and costs (all in *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 2010 U.S. Dist. LEXIS 93644 (D. Maryland 2010)). "When parties and/or their counsel fail in their duty to conduct proper searches of ESI, sanctions may be appropriate, even where the misconduct involves late disclosure, as opposed to spoliation." *Nycomed US Inc. v. Glenmark Generics Ltd.*, 2010 U.S. Dist. LEXIS 82014. The *Nycomed* court warned: "A showing of bad faith on the part of the offending party is not required [for the imposition of sanctions] under Rule 37." Rule 37 (Fed. R. Civ. P. 37(b)(2)) mandates that the court "must order the disobedient party, the attorney advising that party, or both to pay the reasonable expenses, including attorney's fees, caused by the [violation of a discovery order], unless the failure was substantially justified or other circumstances make an award of expenses unjust."

It is difficult to argue for the justification of failure or the existence of other circumstances that would make an award of sanctions unjust if your company or firm, faced with other (and in hindsight, much better) alternatives, decided that it was better to assume all control and risk in the management of eDiscovery compliance.

With the nominal value of "reducing client expenses," outsourcing has received tacit approval within certain guidelines. Those guidelines seem to follow a common-sense approach that requires the same sort of diligence, control and oversight as if the firm's non-attorney in-house staff were doing the work.

The use of third-party experts to provide eDiscovery services is typically the fastest and least risky approach to take in the course of discovery compliance in litigation. A well-qualified eDiscovery service provider has access to experts in the rapidly changing and developing technology that must be used to collect, process the virtual mountains of discoverable ESI, and produce a responsive subset of that ESI that can then be reviewed by legal experts for privilege or other protection from disclosure in the often short time frames that are imposed by our busy court systems.

An added benefit of engaging a third-party to help the company or firm handle eDiscovery matters is the ability to produce a detailed and segregable bill for the costs of handling the eDiscovery

matter. If those costs are awarded to your company or your client, there is a clear and documented accounting for these costs. The difficulty in documenting internal firm eDiscovery costs, and the risk that billing an associate's time as an attorney when that person was conducting non-attorney eDiscovery services could result in overbilling sanctions, are two more reasons why trying to handle eDiscovery in-house may not be such a great idea.

A consulting services provider, who provides a variety of discovery and litigation support services, or who aggregates the services of individual eDiscovery service providers as subcontractors, may provide a reasonable and efficient approach to handling the company's or firm's eDiscovery compliance matters. For the company or law firm without adequate in-house expertise to understand and manage the numerous services and technologies that are available in the litigation support marketplace from numerous service providers, these consulting service providers can be the key to keeping litigation costs in check and to winning a case.

By interposing a competent, careful and respected third-party eDiscovery expert between your company or firm and the possible sanctions that a court could impose upon your company or firm, you can achieve the desired outcome of compliance with the Federal Rules and any discovery orders while helping to insulate your company or firm from sanctions for noncompliance.

It should also be noted that the tried and true practice of custodian based ESI collection is now under fire by courts, which appear to be looking at this practice with an increasing level of distrust. In *Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of America Sec. LLC*, No. 05 Civ. 9016, 2010 U.S. Dist. Lexis 4546, at *1 (S.D.N.Y. Jan. 15, 2010), eDiscovery expert Judge Shira Scheindlin held that some manual collection efforts warranted a sanction for spoliation of evidence because, among other defects, the plaintiffs relied solely on their employees to search and select what they believed to be responsive information without adequate attorney direction and supervision. In *Pension Comm.*, the judge found fault with the Plaintiff's reliance on manual collections:

"This instruction does not meet the standard for a litigation hold. It does not direct employees to preserve all relevant records–both paper and electronic-nor does it create a mechanism for collecting the preserved records so that they can be searched by someone other than the employee. Rather, the directive places total reliance on the employee to search and select what that employee believed to be responsive records without any supervision from Counsel."

The risks of handling technical, time-constrained or extensive eDiscovery tasks in-house are high, and present not only financial risks for the company, but also ethical risks for the law firm. The choice of a qualified, competent and careful third-party eDiscovery service provider to work with the company or law firm provides the most efficient, economical, and safest route through the tangled forest of eDiscovery compliance. For your convenience I have included an article on eDiscovery that may be of some interest to you. Give this some thought and let me know when you would like to discuss it.

Sincerely,

LITIGATION HOLD NOTICE

LEGAL HOLD MEMORANDUM

MEMORANDUM

PRIVILEGED & CONFIDENTIAL
ATTORNEY-CLIENT COMMUNICATION
ATTORNEY WORK PRODUCT

TO: _____

FROM: _____

CC: _____

DATE: _____

SUBJECT: _____

As you may be aware, _____ recently engaged in a legal matter regarding, _____. Both written documents and electronic data contained in _____computer systems are likely to be an important source of discovery and evidence in this lawsuit. As a result, _____ is required to take steps to ensure that all documents and electronic data that are potentially relevant to this lawsuit are preserved. You have been identified as someone who may have potentially relevant documents or electronic data. This notice does not mean that you are necessarily involved in the dispute; however, _____ is now under a legal duty to preserve all evidence, whether in printed or electronic form, that might become relevant to this matter (and to continue to preserve such evidence related to the matter). Some of this information may be in your possession or control, and as an employee, you have a legal duty to preserve that information, even if in the normal course of operations those records could be deleted; to satisfy our legal obligations, we require your assistance in preserving _____ documents and electronic data as described in the following directive.

Directive Regarding Preservation of Documents and Electronic Data

Effective immediately you must preserve and retain, and you must continue to preserve and retain, (*i.e.*, do not alter, delete, destroy, or otherwise modify) any documents or electronic data (including, but not limited to, all e-mails and other electronically stored documents) that are or may be relevant to Mary E. Halbeisen's alleged discrimination. Relevant documents and data include:

- All communications to or from _____;

- All information referring or relating to _____; and
- All information referring or relating to gender discrimination and retaliation, even if it relates to someone other than _____.

Any question you may have as to the relevance of a particular document file, e-mail or other electronic data compilation should be resolved in favor of preservation and retention. Failure to preserve relevant information could result in significant penalties against _____.

The following information might be relevant to the dispute: (*reference specific items as they may relate to the issue at hand*) In identifying and preserving the above documents and data, please keep in mind that documents and electronic data include, but are not limited to, application files, drafts, correspondence, telephone logs, e-mail, text files (including word processing documents and presentations), journal or calendar entries, calendar and scheduling information, task lists, notes, Blackberry messages, voice-mails, spreadsheets, reports, invoices, purchases orders, meeting minutes, working files, databases containing information, computer system activity logs, internet usage files, and network access information. _____ computer systems include, but are not limited to, all workstations, laptops, network servers, removable media, handheld devices, voicemail, and backup tapes. Again, any questions as to the scope of this directive should be resolved in favor of preservation and retention.

You are required to take the following steps immediately to protect and preserve any of the information that is in your possession or under your control until further notice. Specifically:

1. Suspend deletion, overwriting, or any other destruction of electronic information relevant to this dispute. This includes electronic information wherever it is stored – at your workstation, on a laptop, on your cell phone, on an external storage device, such as a thumb-drive, or at home. This includes all forms of electronic communication (e.g. email, word processing, calendars, voice messages, videos, photographs, information on your cell phone or PDA). The information must be preserved in its original electronic form, so that all information contained within it, whether visible or not, is also available for inspection – i.e., it is not sufficient to make a hard copy of electronic communication.

2. For electronic materials, you should create an electronic folder and move all e-mails, word documents, pdfs, other electronically stored data, etc. into that folder. For hard-copy materials, notes, etc., you should put them in a folder in a secure space.

3. Similarly, preserve any new electronic information that is generated after you receive this notice that could be considered relevant to this dispute.

4. Preserve any hard copy under your control.

5. At the network and systems administration level, this directive requires you to preserve and retain all potentially relevant files stored on _____ servers and to refrain from doing any administrative work that has the potential to destroy potentially relevant files. Any "janitorial" functions must be disabled. All backup tapes must be preserved and pulled from recycling rotation for any materials in existence.

Please execute and return to _____, as _____, as soon as possible the attached CERTIFICATION OF RECEIPT AND COMPLIANCE WITH LEGAL HOLD MEMORANDUM, confirming that you have received, read, understand and intend to comply with this directive. This is an important legal duty and failure to follow these instructions may subject you to discipline, as the failure to preserve information has very serious consequences for _____.

Please advise us immediately if you have any questions about, or any problems complying with this Legal Hold Memorandum. Please notify us if you are aware of individuals (other than those listed above) or third parties who may have documentation/information and or should receive this Legal Hold Memorandum.

Thank you for your cooperation.

CERTIFICATION OF RECEIPT AND COMPLIANCE WITH
LEGAL HOLD MEMORANDUM

I hereby certify that I have received a copy of the LEGAL HOLD MEMORANDUM dated [**DATE**] and that I have read and understand the same. I certify that I will comply with the requirements of the LEGAL HOLD MEMORANDUM. I further certify that I will advise Arthur J. Fleischer, Director of Human Resources if I have any questions regarding my duties and responsibilities under the LEGAL HOLD MEMORANDUM or if I become aware of any instances in which I or anyone else fails to comply with the LEGAL HOLD MEMORANDUM.

Signed: _____

Printed Name: _____

Dated: _____

LITIGATION HOLD NOTICE

Date: _____

TO:

Dear _____:

As you know, _____ has a duty to preserve evidence relevant to this action, even without a court order. Because electronic data may be an irreplaceable source of discovery in this matter, it is your client's duty to preserve all potentially relevant electronic data. Furthermore, it is The Law Firm LLP's duty to insure that a proper litigation notification is issued and a litigation hold implemented. Consistent with that duty, we request that your client's data be preserved and maintained – in **native** format, and in accordance with the following safeguards:

1. ELECTRONIC DATA TO BE PRESERVED:

The following types of electronic data and/or the electronic data of your client's subsidiaries, divisions, agents, employees and relevant third-parties or vendors should be preserved in **native** format, in accordance with the steps set forth below:

- All electronic mail and information about electronic mail (including message contents, header and logs of e-mail system usage) sent or received by any custodian relating to the subject matter of the litigation;
- All databases, including field and structural information as well as records, containing any information relating to the subject matter of the litigation;
- All logs of activity on any computer systems that have been used to process or store data containing information relating to the subject matter of the litigation;
- All other electronic data containing information about, or relating to, the subject matter of the litigation, including but not limited to:
  - » All word processing files and file fragments;
  - » Electronic data created by applications which process financial, accounting and billing information;
  - » All electronic calendar and scheduling program files and file fragments;
  - » All electronic spreadsheet files and file fragments.

2. ON-LINE DATA STORAGE

With regard to online storage and/or direct access storage devices including, but not limited to, any file server or data array (e.g. RAID) physically or remotely attached to your client's computers through wired or wireless networking, we request that your client not modify or delete any existing electronic data files that meet the criteria set forth above, unless an exact mirror image has been made and will be preserved and kept accessible for purposes of this litigation.

3. OFF-LINE DATA STORAGE, BACKUPS AND ARCHIVES

With regard to all electronic media used for offline storage, such as magnetic tapes and cartridges, CDs, DVDs, USB devices (e.g. 'thumb drives') and the like, used with any computer, file server or data array (e.g. RAID), whether physically or remotely attached to your client's computers through wired or wireless access that contain any electronic information relating to the subject matter of this litigation, we request that your client stop any activity that may result in the loss of such data. This request is intended to cover all removable electronic media used for data storage in any device, including those containing backup and/or archive data sets.

4. PRESERVATION OF REPLACED DATA STORAGE DEVICES

We request that your client preserve any electronic data storage devices and/or media that may contain data relating to the subject matter of the litigation and that it replaces for any reason.

5. FIXED DRIVES ON STAND-ALONE PERSONAL COMPUTERS AND NETWORK WORKSTATIONS

We request that your client not alter, delete or over-write relevant electronic data that existed on fixed drives attached to stand-alone microcomputers, network workstations and/or data arrays (e.g. RAID) at the time of filing of this action, or perform other procedures such as data compression and disk defragmentation or optimization routines that may impact such data, unless an exact mirror image has been made of such active files and directory listings (including hidden and/or deleted files) for all directories containing such files and that it completely restore any altered, deleted or over-written electronic files and file fragments and arrange to preserve all such data during the pendency of this litigation.

6. APPLICATIONS AND UTILITIES

We request that your client preserve copies of all applications and utilities that may be used to process electronic data discussed in this letter.

7. LOG OF SYSTEM MODIFICATIONS

We request that your client maintain an activity log of document modifications made to any electronic data processing system that may affect any system's capability to process any electronic data relating to the subject matter of the litigation.

8. PERSONAL COMPUTERS AND ALL OTHER DEVICES USED BY EMPLOYEES, INDEPENDENT CONTRACTORS AND OTHERS UNDER THE CONTROL OF YOUR CLIENT

Please immediately take the following steps with regard to all fixed drives attached internally, externally, physically and/or remotely by wired or wireless access to any personal computers used by any custodian under your client's control:

- An exact mirror image must be made of all electronic data relating to the subject matter of the litigation;
- Full directory listings (including hidden and deleted files) for all directories and subdirectories must be written;

Please immediately take the following steps with regard to all removable drives attached internally, externally, physically and/or remotely by wired or wireless access to any personal computers used by any custodian under your client's control:

- All removable electronic media, such as floppy diskettes, magnetic tapes and cartridges, CDs, DVDs, USB devices (e.g. 'thumb drives') and the like that existed before the delivery of this letter and that contain relevant data should collected, maintained intact and kept available during the pendency of this litigation.

Please immediately take the following steps with regard to all other relevant devices used by any custodian under your client's control, whether it is internally, externally, physically and/or remotely attached by wired or wireless access to any system used by your client:

- All cellular phones, personal data assistants (e.g. Blackberry), voicemail messages, text messages (SMS or otherwise), instant messages and/or any other device that stores electronic information (e.g. RAM on printing devices or FAX machines) and the like that existed before the delivery of this letter and that contain relevant data should collected, maintained intact and kept available during the pendency of this litigation.

9. EVIDENCE CREATED AFTER RECEIPT OF THIS LETTER

Any relevant electronic data created after receipt of this letter should be preserved in a manner consistent with the directions in this letter.

10. METADATA

As it is relevant to all items cited hereinabove, your client is instructed to preserve all metadata and not to alter, delete and/or over-write any metadata. Please feel free to contact me to discuss any aspect of this letter.