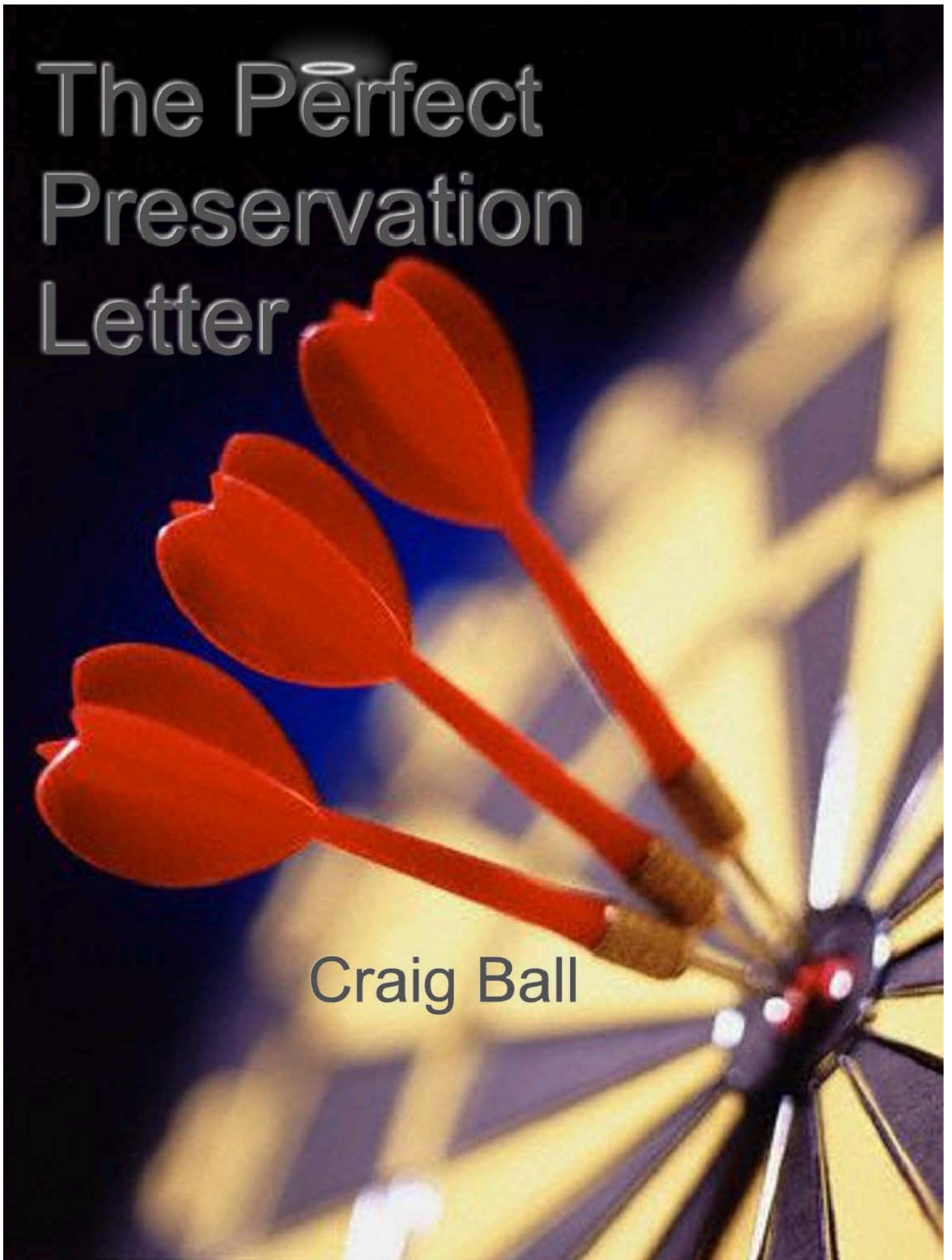


The Perfect Preservation Letter

Craig Ball



The Perfect Preservation Letter

By Craig Ball

**Well, I was drunk the day my Mom got outta prison,
And I went to pick her up in the rain;
But before I could get to the station in my pickup truck,
She got runned over by a damned old train.**

*From "You Never Even Called Me By My Name"
(a/k/a "The Perfect Country and Western Song")
By Steve Goodman, performed by David Allan Coe*

Outlaw musician David Allan Coe sings of how no country and western song can be “perfect” unless it talks of Mama, trains, trucks, prison and getting drunk. Likewise, no digital evidence preservation letter can be “perfect” unless it clearly identifies the materials requiring protection, educates your opponent about preservation options and lays out the consequences of failing to preserve the evidence. *You won’t find the perfect preservation letter in any formbook.* You have to build it, custom-crafted from a judicious mix of technical boilerplate and *fact-specific* direction. It compels broad retention while appearing to ask for no more than the bare essentials. It rings with reasonableness. It keeps the focus of e-discovery where it belongs: relevance. This article discusses features of the perfect preservation letter and offers suggestions as to how it can be effectively drafted and deployed.

Contents

The Role of the Preservation Letter	2
The Proposed Amendments to the Rules of Civil Procedure	2
What is Electronic Evidence Preservation?	3
Touching Data Changes It	3
Digital Evidence Is Increasingly Ill-Suited to Printing	4
Data Must Be Interpreted To Be Used	4
Storage Media Are Fragile and Changing	4
Digital Storage Media Are Dynamic and Recyclable	4
The Duty to Preserve	5
Balance and Reasonableness	5
Preservation Essentials	6
The Nature of the Case	6
When to Send a Preservation Letter	7
Who Gets the Letter?	7
How <i>Many</i> Preservation Letters?	8
Specifying Form of Preservation	8
Special Cases: Back Up Tapes, Computer Forensics and Metadata	8
Back Up Tapes	9
Drive Cloning and Imaging	10
Metadata	11
End Game	12
APPENDIX: Exemplar Preservation Demand to Opponent	13

The Role of the Preservation Letter

“The reality of electronic discovery is it starts off as the responsibility of those who don’t understand the technology and ends up as the responsibility of those who don’t understand the law.”

You can read the Federal Rules of Civil Procedure from cover to cover and not see a reference to preservation letters. So why invest a lot of effort creating the perfect preservation letter? Wouldn’t it be sufficient to remind your opponent that the laws and rules prohibiting destruction of evidence apply to electronically stored information in the same manner that they apply to other evidence and that they must take every reasonable step to preserve this information until the final resolution of the case? Perhaps in a decade or so it will be enough; but, today we face an explosion of electronic evidence untamed by sound records management. Too many litigators and in-house counsel are clueless about information systems. The reality of electronic discovery is it starts off as the responsibility of those who don’t understand the technology and ends up as the responsibility of those who don’t understand the law. A well-drafted preservation letter helps bridge this knowledge gap.

The goal of the preservation letter is, of course, to remind opponents to preserve evidence, to be sure the evidence doesn’t disappear. But, the preservation letter also serves as the linchpin of a subsequent claim for spoliation, helping to establish bad faith and conscious disregard of the duty to preserve relevant evidence. It is today’s clarion call that underpins tomorrow’s, “I told you so.” The more effectively you give notice and convey what must be retained—including methodologies for preservation and consequences of failure--the greater the likelihood your opponent will be punished for destruction of evidence.

The Proposed Amendments to the Rules of Civil Procedure

Though serving a preservation letter isn’t a formal component of civil discovery procedures, it’s likely to be a *de facto* practice as federal and local rules of civil procedure impose express e-discovery “meet and confer” obligations upon litigants. For example, effective December 1, 2006, Rule 26 of the Federal Rules of Civil Procedure will require litigants to “discuss any issues relating to preserving discoverable information,”¹ as well as “any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced.”² The preservation letter is sure to frame the agenda for such discussions.

The preservation letter will may play an important role in a court’s consideration of whether a party acted in good faith in connection with information lost to routine operations of an electronic information system.³ Assessment of good faith turns on the subjective awareness of the party

¹ Proposed Amendment to Rule 26(f) of the Federal Rules of Civil Procedure. All proposed Amendments and commentary cited are available at http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf.

² Id. Rule 26(f)(3)

³ Id. Proposed Rule 37(f), entitled “Electronically Stored Information” provides, “Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.”

failing to preserve evidence. The preservation letter can establish such awareness, bolstering a claim that the party destroying evidence knew of its discoverability and recklessly or intentionally disregarded it. Per commentary to the proposed rule, “Good faith in the routine operation of an information system may involve a party’s intervention to modify or suspend certain features of that routine operation to prevent the loss of information, if that information is subject to a preservation obligation.”⁴ A clear and instructive preservation letter that serves to educate your opponent isn’t just a professional courtesy; it also compels recognition of a duty to intervene to prevent data loss and deprives an opponent of a sanctions “safe harbor.”

“A clear and instructive preservation letter that serves to educate your opponent isn’t just a professional courtesy....”

What is Electronic Evidence Preservation?

When evidence is a paper document, preserving it is simple: We set the original or a copy aside, confident that it will come out of storage exactly as it went in. Absent destructive forces or tampering, paper stays pretty much the same. But despite lawyers’ ardor for paper, 95% of information is born *digitally*, and the overwhelming majority is never printed.

By contrast, preserving electronic data poses unique challenges because:

- “Touching” data changes it
- Digital evidence is increasingly ill-suited to printing
- Data must be interpreted to be used
- Storage media are fragile and changing all the time
- Digital storage media are dynamic and recyclable

Touching Data Changes It

Route a document through a dozen hands and, aside from a little finger grime or odd coffee stain, the document won’t spontaneously change just by moving, copying or reading it. But open that same document in Microsoft Word, or copy it to a CD, and you’ve irretrievably changed that document’s *system metadata*, the data-about-data items, like the document’s creation or last access dates that may themselves be evidence.

It’s common to use recordable CDs to transfer data between systems or as a medium of e-production. But how many lawyers are aware that you *can’t easily* copy all of a file’s metadata when it’s moved from hard drive to a recordable CD? The two media use different file systems such that the CD-R doesn’t offer a structure capable of storing all of a file’s Windows metadata. That is, where the Windows file system offers three slots for storing file dates (i.e., Modified, Accessed and Created), the CD-R file structure has but one. With no place to go, metadata is jettisoned in the CD recording process, and the missing metadata may be misreported on the destination system.

⁴ *Id.* Committee Note to Proposed Rule 37(f).

Digital Evidence Is Increasingly Ill-Suited to Printing

Much modern evidence doesn't lend itself to paper. For example, a spreadsheet displays values derived from embedded formulae, but you can't embed those formulae in paper. In large databases, information occupies expansive grids that wouldn't fit on a printed page or make much sense if it could. And, of course, sound and video evidence can't make the leap to paper. So preserving on paper isn't always an option, and it's rarely an inexpensive or efficient proposition.

Data Must Be Interpreted To Be Used

If legible and in a familiar language, a paper document conveys information directly to the reader. A literate person can interpret an alphabet, aided by blank space and a few punctuation marks. It's a part of our grade school "programming." But *all* digital data are just streams of ones and zeroes. For those streams of data to convey anything intelligible to people, the data must be interpreted by a computer using specialized programming called "applications." Without the right application—sometimes even without the correct *version* of an application—data is wholly inaccessible or may be inaccurately presented. Successfully preserving data also entails preserving legacy *applications* capable of correctly interpreting the data as well as legacy computing environments—hardware and software—capable of running these applications.

Storage Media Are Fragile and Changing

If your great grandfather put a letter in a folder a century ago, chances are good that notwithstanding minor signs of age, you could pull it out today and read it. But changes in storage technology and rapid obsolescence have already rendered fifteen-year-old digital media largely inaccessible absent considerable effort and expense. How many of us still have a computer capable of reading a 5.25" floppy? The common 3.5" floppy disk is disappearing, too, with even CD-ROMs fast on its heels to oblivion. Data stored on back up tapes and other magnetic and even optical media fades and disappears over time like the contents of once-common thermal fax paper. Disks expected to last a century are turning up illegible in a decade. Back up tapes may stretch a bit each time they are used and are especially sensitive to poor storage conditions. Long-term data preservation will entail either the emergence of a more durable medium or a relentless effort to migrate and re-migrate legacy data to new media.

Digital Storage Media Are Dynamic and Recyclable

By and large, paper is not erased and reused for information storage; at least not in a way we'd confuse its prior use as someone's Last Will & Testament with its reincarnation as a cardboard carton. By contrast, a hard drive is constantly changing and recycling its contents. A later version of a document may overwrite—and by so doing, destroy—an earlier draft, and storage space released by the deletion of one file may well be re-used for storage of another. This is in sharp contrast to paper preservation, where you can save a revised printout of a document without affecting—and certainly not obliterating-- a prior printed version.

Clearly, successful preservation of digital data isn't always as simple as copying something and sticking it in a folder; but your opponent may not appreciate the planning and effort digital preservation requires. When that's the case, the requesting party is at a crossroads: Do you seek to educate the producing party or its counsel about how and why to properly preserve

digital evidence, or do you keep mum in hopes that an advantage will flow from your opponent's ineptitude? That is, do you want the evidence or the sanction? Most of the time, you'll want the evidence.

The Duty to Preserve

At what point does the duty to preserve evidence arise? When the lawsuit is filed? Upon receipt of a preservation letter? When served with a request for production?

The duty to preserve evidence may arise before—and certainly arises without—a preservation letter. In fact, the duty can arise long before. A party's obligation to preserve evidence is generally held to arise when the party knows or has reason to know that evidence may be relevant to future litigation. This "reasonable anticipation of litigation" standard means that any person or company who should see a claim or lawsuit on the horizon must act, *even before a preservation letter or lawsuit has materialized*, to cease activities likely to destroy electronic or tangible evidence and must take affirmative steps to preserve such evidence.

Thus, the preservation letter may be only one of a number of events—albeit a decisive one—sufficient to trigger a duty to preserve evidence. Arrival of the preservation letter is often the first time responding parties focus on what evidence exists and what they will elect to save.

Balance and Reasonableness

The problem with preservation letters is that they often must be sent when you know little-to-nothing about your opponent's information systems; consequently, they tend to be everything-but-the-kitchen-sink requests, created without much thought given to the "how" and "how much" issues faced by the other side.

A preservation letter that demands the moon and paralyzes your opponent's operations won't see compliance or enforcement. Absent evidence of misconduct (such as shredding or other overt destruction of evidence), a court isn't likely to sanction a party for failing to comply with a preservation letter so onerous that no one dare turn on their computer for fear of spoliation! For a preservation letter to work, it must be reasonable on its face. Remember: all you're trying to do is keep the other side from destroying relevant evidence, and just about any judge will support you in that effort *if your demands aren't cryptic, overbroad or unduly burdensome*.

If it could be accomplished with paper evidence, judges expect a corollary accomplishment with electronic evidence. Still, digital is different, and some of the ways we approach paper discovery just won't fly for electronic evidence. For example, using the term "any and all" in a request for digital evidence is a red flag for potential over breadth. Demanding that an opponent retain "any and all electronic communications" is nonsense. After all, phone conversations are electronic communications, and it's unlikely that a court would require a litigant to tape all phone calls, though a judge shouldn't hesitate to compel *retention* of the tapes *when phone calls are already recorded and relevant*. If what you want preserved is e-mail, or instant messaging or voice mail, *spell it out*. Your opponent may squawk, but at least the battle lines will be drawn on specific evidentiary items your opponent may destroy instead of fighting about what constitutes a "communication?" The risk to this approach is that your opponent may fail to preserve what you haven't specified. Still, to the extent the evidence destroyed was relevant and material, that

risk may be adequately addressed by a demand to retain all information items bearing on the claims made the basis of the claim. Further, the preservation letter neither creates the duty to preserve nor constrains it. If the evidence was relevant and discoverable, then destroyed at a time when your opponent should have known to keep it, it's still spoliation.

Preservation Essentials

A perfect preservation letter must, first and foremost, seek to halt routine business practices geared to the destruction of potential evidence. It might call for an end to server back up tape rotation (as appropriate), electronic data shredding, scheduled destruction of back up media, re-imaging of drives, drive hardware exchanges, sale, gift or destruction of computer systems and, (especially if you know computer forensics may come into play) disk defragmentation and maintenance routines. A lot of digital evidence disappears because of a lack of communication ("legal forgot to tell IT") or of individual initiative ("this is MY e-mail and I can delete it if I want to"). So, be sure to highlight the need to effectively communicate retention obligations to those with hands-on access to systems, and suggest steps to forestall personal delete-o-thons. **Remember:** When you insist that communications about preservation obligations *reach* every custodian of discoverable data and that such communications stress the importance of the duty to preserve, you are demanding no more than the developing law suggests is warranted. See, e.g., *Zubulake v. UBS Warburg LLC*, No. 02 Civ. 1243 (S.D.N.Y. July 20, 2004) ("*Zubulake V*").

Next, get fact specific! Focus on items specifically bearing on the claim or suit, like relevant business units, activities, practices, procedures, time intervals, jurisdictions, facilities and key players. Here, follow the "who, what, when, where and how" credo of good journalism. Preservation letters are more than a boilerplate form into which you pack every synonym for document and computer in the thesaurus. If your preservation letter boils down to "save everything about anything by everyone, everywhere at any time," it's time to re-draft it because not only will no trial court enforce it, many will see it as discovery abuse.

The preservation letter's leading role is to educate your opponent about the many forms of relevant electronic evidence and the importance of taking prompt, affirmative steps to be sure that evidence remains accessible. Educating the other side isn't a noble undertaking—it's sound strategy. Spoliation is frequently defended on the basis of ignorance; e.g., "Your honor, we had no idea that we needed to do that," and your goal is to slam the door on the "it was an oversight" excuse. Doing so entails more than just reciting a litany of storage media to be preserved--you've got to educate, clearly and concisely.

Finally, don't be so focused on electronic evidence that you fail to direct your opponent to retain the old-fashioned paper variety. And remember that turnabout is fair play. Don't compel your opponent to preserve data to an extent much greater than *your* client could sustain. Doing so could hurt your credibility with the court right out of the gate.

The Nature of the Case

As formal discovery requests come after service of a complaint, the parties know what the dispute is about by the time the discovery requests arrive. But a pre-suit preservation letter may be your opponent's first inkling that they face litigation. Don't just assume that those receiving your preservation letter know what the dispute is about: *spell it out for them*. Though you may

be unprepared to draft your formal complaint, furnish sufficient information about the nature of the case to sustain a later claim that a reasonable person reading the preservation letter would have known to preserve particular evidence. Names of key players, dates, business units, office locations and events will all be weighed in deciding what's relevant and must be retained. The more you can offer, the less likely you are to someday hear, "If you wanted Bob's e-mail, why didn't you mention Bob in the preservation letter?"

When to Send a Preservation Letter

"There may be circumstances where you *want* your opponent's routine destruction of information to continue...."

The conventional wisdom is that preservation letters should go out as soon as you can identify potential defendants. But there may be compelling reasons to delay sending a preservation letter. For example, when you face opponents who won't hesitate to destroy evidence, a preservation letter is just the starting gun and blueprint for a delete-o-thon. Instead, consider seeking a temporary restraining order or the appointment of a special master (but recognize that the Comments to the proposed Rules amendments strongly discourage entry of *ex parte* preservation orders). Delay in sending the letter may be wise when your investigation is ongoing and the service of a preservation letter will cause the other side to hire a lawyer or trigger privileges running from the anticipation of litigation. There may even be circumstances where you *want* your opponent's routine, good faith destruction of information to continue, such as where information unfavorable to your position will be lost in the usual course of business.

Who Gets the Letter?

If counsel hasn't appeared for your opponent, to whom should you direct your perfect preservation letter? Here, the best advice is err on the side of as many appropriate persons as possible. Certainly, if an individual will be the target of the action, he or she should receive the preservation letter. However, if you know of others who may hold potential evidence (such as the defendant's spouse, accountant, employer, banker, customers and business associates), it's smart to serve a preservation demand upon them, making clear that you are also seeking preservation of physical and electronic records in their possession pertaining to the matters made the basis of the contemplated action. Some litigants use the preservation letter as a means to put pressure upon customers lost to or solicited by a competitor-defendant. **Beware**...as the preservation letter isn't a discovery mechanism expressly countenanced by the rules of procedure, its use as an instrument of intimidation may not be privileged and could provoke a counterclaim based on libel or tortious interference.

If the potential defendant is a corporation, a presentation addressed to the wrong person may be ignored or late in reaching those able to place litigation holds on records. Consequently, it's wise to direct preservation letters to several within the organization, including, *inter alia*, the Chief Executive Officer, General Counsel, Director of Information Technologies and perhaps even the Head of Corporate Security and registered agent for service of process. You may want to copy other departments, facilities or business units.

You naturally want to be sure that as many who hold evidence as possible are put on notice, but you also want to disseminate the preservation duty widely to foment uncertainty in those who

might destroy evidence but for the possibility that others in the organization will retain copies. Of course, if counsel has entered an appearance, weigh whether you are constrained from communicating directly with represented parties.

If possible, consider who is most likely to *unwittingly* destroy evidence and be certain that person receives a preservation letter. Sending a preservation letter to a person likely to destroy evidence *intentionally* is a different story. The letter may operate as the triggering event to spoliation, so you may need to balance the desire to give notice against the potential for irretrievable destruction.

Of course, preservation letters, like any important notice, should be dispatched in a way enabling you to prove receipt, like certified mail, return receipt requested.

How *Many* Preservation Letters?

Turning to the obligatory litigation-as-war metaphor, is a preservation letter best delivered as a single giant salvo across the opponent's bow, or might it instead be more effectively launched as several carefully-aimed shots? It's common to dispatch a single, comprehensive request, but might it instead be wiser to present your demands in a *series* of focused requests, broken out by, e.g., type of digital medium, issues, business units, or key players? Your preservation letter may be destined to be an exhibit to a motion, so when the time comes to seek sanctions for a failure to preserve evidence, wouldn't it be more compelling to direct the court to a lean, specific preservation notice than a bloated beast? Also, consider supplementing a "master" preservation notice with specific notices directed at key players as the matter proceeds. It's difficult to claim, "We didn't realize you wanted **Bob's** e-mail" when Bob got his very own, custom-tailored preservation letter.

Specifying Form of Preservation

The proposed amendments to the Federal Rules of Civil Procedure permit a requesting party to specify the form or forms in which the requesting party wants electronic evidence produced. Some states, notably Texas, already permit such a designation in their rules governing discovery. Often, there's no additional trouble or expense for the producing party to generate one format over another and occasionally a non-native production format proves easier or cheaper to manage. But, should the *preservation letter* specify the form in which the data should be preserved? Generally, the answer is "No," because you don't want your preservation letter to appear to demand anything more onerous than maintaining evidence in the way it's kept in the ordinary course of business. On the other hand, when your specification operates to **ease** the cost or burden to the producing party or otherwise **helps** the producing party fulfill its preservation obligation, a format might be *suggested* (although, be clear that the specified form is just one acceptable format).

Special Cases: Back Up Tapes, Computer Forensics and Metadata

The e-discovery wars rage in the mountains of e-mail and flatlands of Excel spreadsheets, but nowhere is the battle so pitched as at the front lines and flanks called *back up tapes, computer forensics and metadata*. These account for much of the bloodshed and so deserve special consideration in a preservation letter.

Back Up Tapes

In the “capture the flag” e-discovery conflicts now waged, the primary objective is often your opponent’s server back up tapes or, more particularly, forcing their retention and restoration. Back up systems have but one legitimate purpose, being the retention of data required to get a business information system “back up” on its feet in the event of disaster. To this end, a business need retain disaster recovery data for a brief interval since there are few instances where a business would wish to re-populate its information systems with stale data. Because only the latest data has much utility in a properly designed back up system, the tapes containing the oldest backed-up information are typically recycled over time. This practice is “tape rotation,” and the interval between use and reuse of a particular tape or set of tapes is the “rotation cycle” or “rotation interval.”

Ideally, the contents of a backup system would be entirely cumulative of the active “online” data on the servers, workstations and laptops that make up a network. But because businesses entrust the power to destroy data to every computer user—including those motivated to make evidence disappear—backup tapes are often the only evidence containers beyond the reach of those with the incentive to destroy or fabricate evidence. Going back to Col. Oliver North’s deletion of e-mail subject to subpoena in the Iran-Contra affair, it’s long been the backup systems that ride to truth’s rescue with “smoking gun” evidence.

Another reason back up tapes lie at the epicenter of e-discovery disputes is that many organizations elect to retain back up tapes for archival purposes (or in response to litigation hold instructions) long after they’ve lost their usefulness for disaster recovery. Here again, when data has been deleted from the active systems, the stale back up tapes are a means (joined by, *inter alia*, computer forensics and discovery from local hard drives) by which the missing pieces of the evidentiary puzzle can be restored.

In organizations with many servers, back up systems are complex, hydra-headed colossi. There may be no simple one-to-one correspondence between a server and a particular user, and most tape back up systems structure stored data differently from active data on the server, complicating restoration and exploration. Volume, complexity and the greater time it takes to access tape compared to disk all contribute to the potentially high cost of targeting back up tapes in discovery. Compelling a large organization to interrupt its tape rotation, set aside back up tapes and purchase a fresh set can carry a princely price tag, but if the tapes aren’t preserved, deleted data may be gone forever. This is the Hobson’s choice⁵ of e-discovery.

A preservation letter should target just the backup tapes likely to contain deleted data relevant to the issues in the case—a feat easier said than done. Whether by Internet research, contact with former employees or consultation with other lawyers who’ve plowed the same ground, seek to learn all you can about the architecture of the active and backup systems. The insight gleaned from such an effort may allow for a more narrowly tailored preservation request or justify a much broader one.

⁵ Thomas Hobson was a British stable keeper in the mid-1600s whose policy was that you either took the horse nearest the stable door or he wouldn’t rent you a horse. “Hobson’s choice” has come to mean an illusory alternative. Back up tapes are problematic, but the unacceptable alternative is letting evidence disappear.

The responding party need not retain purely cumulative evidence, so once established that data has not been deleted and all relevant information still exists on the servers, the back up tapes should be released to the rotation. Again, this is a goal more easily stated than achieved because it requires three elements too often absent from the adversarial process: **communication, cooperation and trust**. Hopefully, the advent of compulsory meet-and-confer sessions will force litigants to focus on e-discovery issues sufficiently early to stem unnecessary costs by narrowing the breadth of preservation efforts to just those actions or items most likely to yield discoverable data.

Drive Cloning and Imaging

Data deleted from a personal computer isn't gone. The operating system simply releases the space the data occupies for reuse and treats the space as available for reuse. Deletion rarely erases data. In fact, there are three and *only* three ways that information's destroyed on personal computer:

1. Completely overwriting the deleted data on magnetic media (e.g., floppy disks, tapes or hard drives) with new information;
2. Strongly encrypting the data and then "losing" the encryption key; or,
3. Physically damaging the media to such an extent that it cannot be read.

There are three and *only* three ways that information's destroyed on a personal computer

Computer forensics is the name of the science that, *inter alia*, resurrects deleted data. Because operating systems turn a blind eye to deleted data (or at least that which has gone beyond the realm of the Recycle Bin), a copy of a drive made by ordinary processes won't retrieve the sources of deleted data. Computer forensic scientists use specialized tools and techniques to copy every sector on a drive, including those holding deleted information. When the stream of data containing each bit on the media (the so-called "bitstream") is duplicated to another drive, the resulting forensically qualified duplicate is called a "clone." When the bitstream's stored in files, it's called a "drive image." Computer forensic tools analyze and extract data from both clones and images.

In routine computer operation, deleted data is overwritten by random re-use of the space it occupies or by system maintenance activities; consequently, the ability to resurrect deleted data with computer forensics erodes over time. When the potential for discovery from deleted files on personal computers is an issue, a preservation letter may specify that the computers on which the deleted data reside should be removed from service and shut down or imaged in a forensically sound manner. Such a directive might read:

You are obliged to take affirmative steps to prevent anyone with access to your data, systems and archives from seeking to modify, destroy or hide electronic evidence on network or local hard drives (such as by deleting or overwriting files, using data shredding and overwriting applications, defragmentation, re-imaging or replacing drives, encryption, compression, steganography or the like). With respect to workstation and laptop hard drives, one way to protect existing data on

is the creation and authentication of a forensically-qualified image of all sectors of the drive. Such a forensically-qualified duplicate may also be called a bitstream image or clone of the drive. Be advised that a conventional back up or “Ghosting” of a hard drive are not forensically-qualified procedures because they capture only active data files and fail to preserve forensically-significant data that may exist in such areas as unallocated space, slack spaces and the swap file.

For the hard drives and other digital storage devices of each person named below, and of each person acting in the capacity or holding the job title named below, as well as each other person likely to have information pertaining to the instant action on their computer hard drive(s) or other electronic storage media, demand is made that you immediately obtain, authenticate and preserve forensically-qualified images of the hard drives and other storage media in (or used in conjunction with) any computer system (including portable and home computers) used by that person during the period from ____ to _____, as well as recording and preserving the system time and date of each such computer.

[Insert names, job descriptions and titles here].

Once obtained, each such forensically-qualified image should be labeled to identify the date of acquisition, the person or entity creating the image, the deviation (if any) of the system time and date and the system from which it was obtained. Each such image should be preserved without alteration.

Be advised that booting a drive or other electronic storage media, examining its contents or running any application will irretrievably alter the evidence it contains and may constitute unlawful spoliation of evidence.

Metadata

Metadata, the “data about data” created by computer operating systems and applications, may be critical evidence in your case, and its preservation requires prompt and definite action. Information stored and transmitted electronically must be tracked by the system which stores it and often by the application that creates it.

For example, a Microsoft Word document is comprised of information you can see (e.g., the text of the document and the data revealed when you look at the document’s “Properties” in the File menu), as well as information you can’t see (e.g., tracked changes, revision histories and other data the program uses internally). This *application* metadata is stored as part of the document file and moves with the file when it is copied or transmitted. In contrast, the computer system on which the document resides keeps a record of when the file was created, accessed and modified, as well as the size, name and location of the file. This *system* metadata is typically not stored within the document, at least not completely. So when a file is copied or transmitted—as when it’s burned to disk for production—potentially relevant and discoverable system metadata is not preserved or produced. Worse, looking at the document or copying it may irreparably alter the metadata. Absent proper steps to protect metadata, even a virus scan can corrupt metadata evidence.

Metadata is not a critical element in all disputes, but in some the issue of *when* a document or record was created, altered or copied lies at the very heart of the matter. If you reasonably anticipate that metadata will be important, be sure to direct the producing party to preserve relevant metadata evidence and warn of the risks threatening corruption. Because many aren't aware of metadata—and even those who are may think of it just in the context of application metadata—the preservation letter needs to define metadata and educate your opponent about where to find it, the common operations that damage it and, if possible, the means by which it's preserved.

For further information about metadata, see “*Beyond Data about Data: the Litigators Guide to Metadata*” at <http://www.craigball.com/metadata.pdf>.

End Game

Are you prepared to let relevant evidence disappear without a fight? **No!**
Can the perfect preservation letter really make *that* much difference? **Yes!**

The preservation letter demands your best effort for a host of reasons. It's the basis of your opponent's first impression of you and your case. A well-drafted preservation letter speaks volumes about your savvy, focus and preparation. An ill-drafted, scattergun missive suggests a formbook attorney who's given little thought to where the case is going. A letter that demonstrates close attention to detail and preemptively slams the door on cost-shifting and “innocent” spoliation bespeaks a force to be reckoned with and signals a case that deserves to be a settlement priority. The carefully-crafted preservation letter serves as a blueprint for meet and confer sessions and a touchstone for efforts to remedy destruction of evidence.

Strategically, the preservation letter forces your opponent to weigh potential costs and business disruption at the outset, often before a lawsuit is filed. If it triggers a litigation hold, everyone from the board room to the mail room may learn of the claim and be obliged to take immediate action. It may serve as the starting gun for a reckless delete-o-thon or trigger a move toward amicable resolution. But done right, ***the one thing it won't be is ignored.***

Craig Ball (craig@ball.net) is a Texas trial lawyer, court-appointed Special Master in matters of electronic evidence and a certified computer forensic examiner. A frequent speaker and author, his e-discovery column, “Ball in Your Court” appears monthly in the American Lawyer Media publication, Law Technology News (www.lawtechnews.com).

APPENDIX: Exemplar Preservation Demand to Opponent

What follows *isn't* the perfect preservation letter *for your case*, so I don't recommend adopting it as a form. I include it here as a drafting aid and to flag issues unique to EDD. You should tailor *your* electronic discovery efforts to the issues, parties and systems in your case. Be thorough insofar as data may be relevant, but eschew the "everything and the kitchen sink" approach. Use common sense. If your preservation demand effectively requires your opponent to pull the plug on every computer, what good is it? If you can't articulate *why* particular ESI is potentially relevant, perhaps you shouldn't demand its preservation. CDB

Demand for Preservation of Electronically Stored Information

Plaintiffs demand that you preserve all documents, tangible things and electronically stored information potentially relevant to the issues in this cause. As used in this document, "you" and "your" refers to **[NAME OF DEFENDANT]**, and its predecessors, successors, parents, subsidiaries, divisions or affiliates, and their respective officers, directors, agents, attorneys, accountants, employees, partners or other persons occupying similar positions or performing similar functions.

You should anticipate that much of the information subject to disclosure or responsive to discovery in this matter is stored on your current and former computer systems and other media and devices (including personal digital assistants, voice-messaging systems, online repositories and cell phones).

Electronically stored information (hereinafter "ESI") should be afforded the broadest possible definition and includes (by way of example and not as an exclusive list) potentially relevant information electronically, magnetically or optically stored as:

- Digital communications (e.g., e-mail, voice mail, instant messaging);
- Word processed documents (e.g., Word or WordPerfect documents and drafts);
- Spreadsheets and tables (e.g., Excel or Lotus 123 worksheets);
- Accounting Application Data (e.g., QuickBooks, Money, Peachtree data files);
- Image and Facsimile Files (e.g., .PDF, .TIFF, .JPG, .GIF images);
- Sound Recordings (e.g., .WAV and .MP3 files);
- Video and Animation (e.g., .AVI and .MOV files);
- Databases (e.g., Access, Oracle, SQL Server data, SAP);
- Contact and Relationship Management Data (e.g., Outlook, ACT!);
- Calendar and Diary Application Data (e.g., Outlook PST, Yahoo, blog tools);
- Online Access Data (e.g., Temporary Internet Files, History, Cookies);
- Presentations (e.g., PowerPoint, Corel Presentations)
- Network Access and Server Activity Logs;
- Project Management Application Data;
- Computer Aided Design/Drawing Files; and,
- Back Up and Archival Files (e.g., Zip, .GHO)

ESI resides not only in areas of electronic, magnetic and optical storage media reasonably accessible to you, but also in areas you may deem *not* reasonably accessible. You are obliged to *preserve* potentially relevant evidence from *both* these sources of ESI, even if you do not anticipate *producing* such ESI.

The demand that you preserve both accessible and inaccessible ESI is reasonable and necessary. Pursuant to amendments to the Federal Rules of Civil Procedure that have been approved by the United States Supreme Court (eff. 12/1/06), you must identify all sources of ESI you decline to produce and demonstrate to the court why such sources are not reasonably accessible. For good cause shown, the court may then order production of the ESI, even if it finds that it is not reasonably accessible. Accordingly, even ESI that you deem reasonably inaccessible *must be preserved in the interim* so as not to deprive the plaintiffs of their right to secure the evidence or the Court of its right to adjudicate the issue.

Preservation Requires Immediate Intervention

You must act immediately to preserve potentially relevant ESI including, without limitation, information with the *earlier* of a Created or Last Modified date on or after [DATE] through the date of this demand and concerning:

1. The events and causes of action described in [Plaintiffs' Complaint];
2. ESI you may use to support claims or defenses in this case;
3.
4.

Adequate preservation of ESI requires more than simply refraining from efforts to destroy or dispose of such evidence. You must also intervene to prevent loss due to routine operations and employ proper techniques and protocols suited to protection of ESI. *Be advised that sources of ESI are altered and erased by continued use of your computers and other devices.* Booting a drive, examining its contents or running any application will irretrievably alter the evidence it contains and may constitute unlawful spoliation of evidence. Consequently, alteration and erasure may result from your failure to act diligently and responsibly to prevent loss or corruption of ESI.

Nothing in this demand for preservation of ESI should be understood to diminish your concurrent obligation to preserve document, tangible things and other potentially relevant evidence.

Suspension of Routine Destruction

You are directed to immediately initiate a litigation hold for potentially relevant ESI, documents and tangible things, and to act diligently and in good faith to secure and audit compliance with such litigation hold. You are further directed to immediately identify and modify or suspend features of your information systems and devices that, in routine operation, operate to cause the loss of potentially relevant ESI. Examples of such features and operations include:

- Purging the contents of e-mail repositories by age, capacity or other criteria;
- Using data or media wiping, disposal, erasure or encryption utilities or devices;

- Overwriting, erasing, destroying or discarding back up media;
- Re-assigning, re-imaging or disposing of systems, servers, devices or media;
- Running antivirus or other programs effecting wholesale metadata alteration;
- Releasing or purging online storage repositories;
- Using metadata stripper utilities;
- Disabling server or IM logging; and,
- Executing drive or file defragmentation or compression programs.

Guard Against Deletion

You should anticipate that your employees, officers or others may seek to hide, destroy or alter ESI and act to prevent or guard against such actions. Especially where company machines have been used for Internet access or personal communications, you should anticipate that users may seek to delete or destroy information they regard as personal, confidential or embarrassing and, in so doing, may also delete or destroy potentially relevant ESI. This concern is not one unique to you or your employees and officers. It's simply an event that occurs with such regularity in electronic discovery efforts that any custodian of ESI and their counsel are obliged to anticipate and guard against its occurrence.

[OPTIONAL PARAGRAPHS]

Preservation by Imaging

You should take affirmative steps to prevent anyone with access to your data, systems and archives from seeking to modify, destroy or hide electronic evidence on network or local hard drives (such as by deleting or overwriting files, using data shredding and overwriting applications, defragmentation, re-imaging or replacing drives, encryption, compression, steganography or the like). With respect to local hard drives, one way to protect existing data on local hard drives is by the creation and authentication of a forensically qualified image of all sectors of the drive. Such a forensically qualified duplicate may also be called a bitstream image or clone of the drive. Be advised that a conventional back up of a hard drive is not a forensically qualified image because it only captures active, unlocked data files and fails to preserve forensically significant data that may exist in such areas as unallocated space, slack space and the swap file.

With respect to the hard drives and storage devices of each of the persons named below and of each person acting in the capacity or holding the job title named below, as well as each other person likely to have information pertaining to the instant action on their computer hard drive(s), demand is made that you immediately obtain, authenticate and preserve forensically qualified images of the hard drives in any computer system (including portable and home computers) used by that person during the period from ____ to _____, as well as recording and preserving the system time and date of each such computer.

[Insert names, job descriptions and titles here].

Once obtained, each such forensically qualified image should be labeled to identify the date of acquisition, the person or entity acquiring the image and the system and medium from which it was obtained. Each such image should be preserved without alteration.

Preservation in Native Form

You should anticipate that certain ESI, including but not limited to spreadsheets and databases, will be sought in the form or forms in which it is ordinarily maintained. Accordingly, you should preserve ESI in such native forms, and you should not select methods to preserve ESI that remove or degrade the ability to search your ESI by electronic means or make it difficult or burdensome to access or use the information efficiently in the litigation.

You should additionally refrain from actions that shift ESI from reasonably accessible media and forms to less accessible media and forms if the effect of such actions is to make such ESI not reasonably accessible

Metadata

You should further anticipate the need to disclose and produce system and application metadata and act to preserve it. System metadata is information describing the history and characteristics of other ESI. This information is typically associated with tracking or managing an electronic file and often includes data reflecting a file's name, size, custodian, location and dates of creation and last modification or access. Application metadata is information automatically included or embedded in electronic files but which may not be apparent to a user, including deleted content, draft language, commentary, collaboration and distribution data and dates of creation and printing. Be advised that metadata may be overwritten or corrupted by careless handling or improper steps to preserve ESI. For electronic mail, metadata includes all header routing data and Base 64 encoded attachment data, in addition to the To, From, Subject, Received Date, CC and BCC fields.

Servers

With respect to servers like those used to manage electronic mail (e.g., Microsoft Exchange, Lotus Domino) or network storage (often called a user's "network share"), the complete contents of each user's network share and e-mail account should be preserved. There are several ways to preserve the contents of a server depending upon, e.g., its RAID configuration and whether it can be downed or must be online 24/7. If you question whether the preservation method you pursue is one that we will accept as sufficient, please call to discuss it.

Home Systems, Laptops, Online Accounts and Other ESI Venues

Though we expect that you will act swiftly to preserve data on office workstations and servers, you should also determine if any home or portable systems may contain potentially relevant data. To the extent that officers, board members or employees have sent or received potentially relevant e-mails or created or reviewed potentially relevant documents away from the office, you must preserve the contents of systems, devices and media used for these purposes (including not only potentially relevant data from portable and home computers, but also from portable thumb drives, CD-R disks and the user's PDA, smart phone, voice mailbox or other forms of ESI storage.). Similarly, if employees, officers or board members used online or browser-based e-mail accounts or services (such as AOL, Gmail, Yahoo Mail or the like) to send or receive potentially relevant messages and attachments, the contents of these account mailboxes (including Sent, Deleted and Archived Message folders) should be preserved.

Ancillary Preservation

You must preserve documents and other tangible items that may be required to access, interpret or search potentially relevant ESI, including logs, control sheets, specifications, indices, naming protocols, file lists, network diagrams, flow charts, instruction sheets, data entry forms, abbreviation keys, user ID and password rosters or the like.

You must preserve any passwords, keys or other authenticators required to access encrypted files or run applications, along with the installation disks, user manuals and license keys for applications required to access the ESI.

You must preserve any cabling, drivers and hardware, other than a standard 3.5" floppy disk drive or standard CD or DVD optical disk drive, if needed to access or interpret media on which ESI is stored. This includes tape drives, bar code readers, Zip drives and other legacy or proprietary devices.

Paper Preservation of ESI is Inadequate

As hard copies do not preserve electronic searchability or metadata, they are not an adequate substitute for, or cumulative of, electronically stored versions. If information exists in both electronic and paper forms, you should preserve both forms.

Agents, Attorneys and Third Parties

Your preservation obligation extends beyond ESI in your care, possession or custody and includes ESI in the custody of others that is subject to your direction or control. Accordingly, you must notify any current or former agent, attorney, employee, custodian or contractor in possession of potentially relevant ESI to preserve such ESI to the full extent of your obligation to do so, and you must take reasonable steps to secure their compliance.

System Sequestration or Forensically Sound Imaging

We suggest that, with respect to **[NAME KEY PLAYERS]** removing their ESI systems, media and devices from service and properly sequestering and protecting them may be an appropriate and cost-effective preservation step.

In the event you deem it impractical to sequester systems, media and devices, we believe that the breadth of preservation required, coupled with the modest number of systems implicated, dictates that forensically sound imaging of the systems, media and devices is expedient and cost effective. As we anticipate the need for forensic examination of one or more of the systems and the presence of relevant evidence in forensically accessible areas of the drives, we demand that you employ forensically sound ESI preservation methods. Failure to use such methods poses a significant threat of spoliation and data loss.

By "forensically sound," we mean duplication, for purposes of preservation, of all data stored on the evidence media while employing a proper chain of custody and using tools and methods that make no changes to the evidence and support authentication of the duplicate as a true and complete bit-for-bit image of the original. A forensically sound preservation method guards against changes to metadata evidence and preserves all parts of the electronic evidence, including in the so-called "unallocated clusters," holding deleted files.

Preservation Protocols

We are desirous of working with you to agree upon an acceptable protocol for forensically sound preservation and can supply a suitable protocol, if you will furnish an inventory of the systems and media to be preserved. Else, if you will promptly disclose the preservation protocol you intend to employ, perhaps we can identify any points of disagreement and resolve them. A successful and compliant ESI preservation effort requires expertise. If you do not currently have such expertise at your disposal, we urge you to engage the services of an expert in electronic evidence and computer forensics. Perhaps our respective experts can work cooperatively to secure a balance between evidence preservation and burden that's fair to both sides and acceptable to the Court.

Do Not Delay Preservation

I'm available to discuss reasonable preservation steps; however, *you should not defer preservation steps pending such discussions if ESI may be lost or corrupted as a consequence of delay.* Should your failure to preserve potentially relevant evidence result in the corruption, loss or delay in production of evidence to which we are entitled, such failure would constitute spoliation of evidence, and we will not hesitate to seek sanctions.

Confirmation of Compliance

Please confirm by **[DATE]**, that you have taken the steps outlined in this letter to preserve ESI and tangible documents potentially relevant to this action. If you have not undertaken the steps outlined above, or have taken other actions, please describe what you have done to preserve potentially relevant evidence.

Respectfully,