# Software Development Contract Litigation


Prepared by:
Geoffrey S. Kercsmar, Kercsmar & Feltus PLLC
Daniel J. Noblitt, The Noblitt Group, PLLC


LORMAN®


Published on www.lorman.com - February 2020

INTRODUCING

Lorman's New Approach to Continuing Education

# ALL-ACCESS PASS

## The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 110+ live webinars added every month
- ☑ **Unlimited OnDemand and MP3 Downloads** - Over 3,800 courses available
- ☑ **Videos** - More than 1,900 available
- ☑ **Slide Decks** - More than 3,000 available
- ☑ **White Papers** - More than 1,900 available
- ☑ **Reports**
- ☑ **Articles**
- ☑ **... and much more!**

## Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

## Get Your All-Access Pass Today!

# SAVE 20%

Learn more: **www.lorman.com/pass/?s=special20**

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

## SOFTWARE CONTRACT LITIGATION

### A. Expectations in litigation

1. **Fees and costs—**Many contracts contain fee shifting provisions. These provisions allow the winner in any litigation or arbitration to recover the attorney's fees expended from the other side.

    a. Courts almost always uphold these provisions (often citing the Federal Arbitration Act, 9 U.S.C.A. §§ 1-14). Arbitrators nearly universally do.

    b. Such provisions change the dynamic of litigation immensely. They should always be considered before pursuing a dispute.

        (1) Example: Consider a purchase of software that costs the purchasing company $250,000 in product and consulting costs. A lawsuit, carried through trial or arbitration, could easily exceed $100,000 in legal fees. The purchaser must understand that it could recover $250,000, plus get back the $100,000 it expended in fees. ***Or*** it could lose the lawsuit, in doing so pay its lawyers $100,000, and then be forced to pay out $100,000 to the other side (negative $200,000)—a swing of $450,000.

    c. In addition to contractual fee shifting provisions, several states have statutory provisions that allow the victor in contract litigation to recover its legal fees. Examples include Arizona, Texas and Oklahoma.

        (1) Cites: A.R.S. § 12-341.01 (Arizona; applies to cases arising from contracts); Tex. Civ. Prac. & Rem. Code Ann. § 38.001 (Texas; applies to cases arising from contracts, among other things); Idaho Code Ann. § 12-120 (1) (Idaho; applies only to cases involving $35,000 or less); 12 Okla. Stat. Ann. Tit. 12, § 936 (Oklahoma; applies to cases involving "labor or services" or "or on an open account, a statement of account, account stated, note, bill, negotiable instrument, or contract relating to the purchase or sale of goods, wares, or merchandise"); Nev. Rev. Stat. Ann. § 18.010 (Nevada; plaintiff may recover fees if total recovery is under $20,000, if written instrument or agreement entitles the prevailing party to an award of fees, or if authorized by specific statute); Alaska R. Civ. P. 82 (Alaska; awards attorneys' fees to prevailing party).

(2) These provisions tend to be enforced less rigidly than contractual fee shifting provisions, but typically have the same effect on litigation strategy.

2. **Litigation Discovery—**"Discovery" describes the process wherein the parties in a lawsuit or arbitration ask the other parties (or third parties) for information or documents about the events in dispute.

a. Discovery tools include written interrogatories (written questions), depositions (oral questions), and subpoenas (among other legal procedures).

b. Perhaps the most important dynamic of software and technology litigation is that it is ***fact-intensive***. There is a significant "he-said-she-said" among the salesmen, project managers and engineers of the various parties.

c. Discovery is generally time-consuming and therefore expensive. In highly-technical cases, like software and intellectual property cases, it is exponentially so.

(1) This is often because the lawyers themselves must become familiar with the software and/or technology to intelligently pursue discovery of the other parties' positions.

d. Parties often believe that lawyers conduct the litigation on their own. But the employees are heavily involved too. The employees must educate the lawyers about the software and technology, as well as the facts of the dispute in question. Employees must also attend certain procedures, like depositions and mediations.

e. **Electronic discovery obligations/litigation holds**—Much of the information in any software sale is electronic. All of that information must be made available to other parties upon proper demand. Therefore, the information must be preserved.

(1) The 2015 Amendment to the Federal Rules of Civil Procedure Rule 37(e) essentially reversed the holding from *Zubulake* that litigation holds must be issued.

(a) Courts in different circuits had developed different standards, rules and penalties regarding the preservation of electronically stored information. Amended Rule 37(e) was intended to provide uniformity and predictability.

(2) At the outset of a dispute—not necessarily the filing of a lawsuit—all **relevant** documents (electronic or otherwise) must be saved, even if the normal procedure of the party would be to destroy or delete the information on a periodic basis. This is called a "litigation hold." [SEE APPENDIX C & D FOR SAMPLE LETTERS TO AN OPPOSING PARTY AND TO CLIENTS]

(3) But since the 2015 amendment, formal litigation holds are no longer mandatory in order to avoid sanctions for spoliation of evidence. Rather, they are viewed as evidence that a party took **reasonable** steps to preserve all potentially relevant electronically stored information. The 2015

(4) In addition, negligence and even gross negligence in the loss of electronically stored information no longer warrant adverse inference instructions.

(a) Cite: *CAT3, LLC v. Black Lineage, Inc.*, 164 F. Supp. 3d 488, 496 (S.D.N.Y. 2016). ("The new rule places no greater substantive obligation on the party preserving ESI. Rather, Rule 37(e) does not purport to create a duty to preserve. The new rule takes the duty as it is established by case law, which uniformly holds that a duty to preserve arises when litigation is reasonably anticipated.")

**(b) Guidance from Rule 37(e) 2015 Amendment:**

(i) **When does the duty to preserve attach?** "Courts should consider the extent to which a party was on notice that litigation would be likely and that the information would be relevant. A variety of events may alert a party to the prospect of litigation. Often these events provide only limited information about that prospective litigation, however, so that the scope of the information that should be preserved may remain uncertain. It is important not to be blinded to this reality by hindsight arising from familiarity with the action as it is actually filed. Although the rule focuses on the common-law obligation to preserve in the anticipation or conduct of litigation, courts may sometimes consider whether there was an independent requirement that the lost information be preserved. Such requirements arise from many sources – statutes, administrative regulations, an order in another case, or a party's own information-retention protocols."

(ii) In addition, courts may consider the relative sophistication of the parties and their familiarity with preservation duties. For example, a large corporation that is involved in litigation frequently may very well be held to a higher standard than an individual who has never been involved in litigation before. *See* Fed. R. Civ. P. 37(e) advisory committee's note to 2015 amendment.

(iii) **What is the scope of the duty to preserve?** Due to the ever-increasing volume of electronically stored information and the multitude of devices that generate such information, perfection in preserving all relevant electronically stored information is often impossible. Litigants have a duty to take **reasonable** steps to preserve all information they know or reasonably should know is relevant in the anticipation or conduct of litigation.

(iv) **What is the relevant inquiry for determining whether a party failed to satisfy its duty to preserve?** There are four questions, each of which must be answered in the affirmative, for the party to have failed to satisfy its duty to preserve: (1) Was the information electronically stored information? (2) Should it have been preserved in anticipation or conduct of litigation? (3) Was it lost because a party failed to take reasonable steps to preserve it? (4) Is the lost information such that it cannot be restored or replaced through additional discovery? If the answer to **any** of those four questions is "no," the court cannot move further under Rule 37(e). If the answer to all four is yes, the court must make an additional inquiry to determine which sanctions are appropriate.

(v) **What must be retained?** A single copy of all relevant documents existing at the time the duty is trigger and any relevant documents created thereafter. The method of preservation is up to the producing party: "In recognition of the fact that there are many ways to manage electronic data, litigants are free to choose how this task is accomplished."

(vi) **What are the possible penalties that can be imposed for failing to satisfy this duty?** Upon finding prejudice to a party due to the loss of information, the court may take measures no greater than to cure the prejudice. These do *not* include things such as adverse inference instructions or dismissals; those require something more. Only upon finding that the party who lost the information did so with the intent to deprive the other party of the use of the information in litigation, the court may, at its discretion: (1) presume the information was unfavorable to the party that lost it; (2) give a permissive or mandatory adverse inference jury instruction; or (3) dismiss the action or enter a default judgment.

(5) Other Cases: *Automated Solutions Corp. v. Paragon Data Sys., Inc.,* 756 F.3d 504, 513-14 (6th Cir. 2014) (no duty to preserve daily back-up tapes in a copyright infringement action where the backup tapes were re-written daily and used for disaster recovery instead of an archive in the normal course of business); *AAB Joint Venture v. United States,* 75 Fed. Cl. 432, 443 (2007) (court ordered a "phased approach" where portions of back-up tapes were produced for evaluation to determine if additional restoration was warranted and whether cost-shifting or cost-sharing should be imposed); *Micron Tech., Inc. v. Rambus Inc.,* 645 F.3d 1311, 1320 (Fed. Cir. 2011) (the duty to begin preserving evidence is based on an objective standard; the point at which litigation is 'reasonably foreseeable' is a flexible, fact-specific standard).*CAT3, LLC v. Black Lineage, Inc.*, 164 F.Supp.3d 488, 500 (S.D.N.Y. 2016) ("The emails are plainly 'electronically stored information.' There is no dispute that the plaintiffs were obligated to preserve them in connection with this litigation. As discussed above, information was 'lost' and cannot adequately be 'restored or replaced.' And the plaintiffs' manipulation of the email addresses is not consistent with taking 'reasonable steps' to preserve the evidence."); *Culhane v. Wal-Mart Supercenter*, 364 F.Supp.3d 768, 775 (E.D. Mich. 2019) (providing defendants the chance to withdraw affirmative defenses to avoid mandatory adverse inference instruction because of willful failure to save security camera footage of incident central to the litigation); *Alabama Aircraft Indus., Inc. v. Boeing Co.*, 319 F.R.D. 730, 747-48 (N.D. Ala. 2017), *motion to certify appeal denied*, No. 2:11-CV-03577-RDP, 2017 WL 4572484 (N.D. Ala. Apr. 3, 2017) (granting motion for sanctions in the form of permissive adverse inference instruction where circumstantial evidence could lead a reasonable jury to conclude that defendant's agents acted with intent to deprive plaintiff of use of ESI in litigation).

(a) Cites: *Fujitsu Ltd. V. Fed. Ex. Corp.,* 247 F.3d 423, 436, (2d. Cir. 2001) (sanction for spoliation are decided on a case-by-case basis); *W. v. Goodyear Tire & Rubber Co.,* 167 F.3d 776, 779 (2d Cir. 1999); *Konstantopoulos v. Westvaco Corp.,* 112 F.3d 710, 719-21 (3d Cir. 1997)(expert witness testimony excluded as a sanction for destruction of evidence).

f. Electronic documents are often contained in massive databases. The sifting of relevant documents from irrelevant documents (like e-mails) is a huge undertaking. Outside technology consultants are often hired to sift electronic documents—at a premium rate.

3. **Expert witnesses** are often necessary in technology litigation to explain to the judge and jury how the technology works. Again, expert fees can be exorbitant, as a great deal of time is needed to fully understand the facts in dispute. But if a trial may result, the side with the more effective may prevail—making the cost worthwhile.

4. **Dispositive motions** (such as motions to dismiss and motions for summary judgment) are rarely successful in this type of litigation. The disputes are so fact-dependent, neither party can meet the applicable standards.

5. **Trials** of these cases almost never happen. If they do, you can expect a very costly battle that will take many witnesses. If you have to try a technology case, come prepared and focus your resources—especially the decision-makers' time and attention.

## B. Effective strategies

1. **Manage expectations of parties**—As an attorney, the client's expectations must be managed. There is rarely a clear-cut victory possible.

   a. 92.5% of all civil litigation settles, according to the American Bar Association. In software and technology disputes, the figure is likely higher due to the complexity and litigation costs involved.

   b. Typically, the plaintiff's strategy is to "share the pain": cost-overruns and disappointing initial returns from the technology result in "buyer's remorse."

      (1) Often, the sponsor of the purchase was not the decision-maker. The sponsor is often held responsible for cost over-runs or inefficiency by the decision-makers, and will seek a substitute responsible party. That substitute is typically the seller or implementer of the technology.

2. **Front-load discovery**—Software and technology litigation is fact-intensive. There are entire teams of engineers that must be interviewed by both sides. Many documents—paper and electronic—must be reviewed by both sides. The best strategy is to allow the attorneys to sift through this information to get the clearest picture of the dispute that is possible.

(1) This strategy is **expensive**—but far less expensive than discovering just before trial that the other side is going to win. Lawyers cannot advise clients unless the lawyers fully understand the events that led to the litigation.

3. **Seek mediation**—Mediation, when the parties understand the fact and what is at stake, and participate in good faith, is an amazing tool.

(1) **There is no reason to wait until a lawsuit is filed or arbitration is demanded—mediation is just as useful before a lawsuit as after one is filed.**

(2) The only requirement is that the parties have exchanged enough information to understand the facts and risks involved.

## APPENDIX C

**Litigation Hold Letter to Opposing Counsel/Parties:**

[DATE]

**VIA E-MAIL AND FIRST CLASS MAIL**

[OPPOSING COUNSEL]
[OPPOSING COUNSEL'S LAW FIRM]
[ADDRESS]
[ADDRESS]

Re: *[CASE NAME]*

Dear _____:

By this letter, you and your clients are hereby given notice not to destroy, conceal or alter any paper or electronic files and other data generated by or stored on [YOUR CLIENTS'] computers and storage media (*e.g.*, hard disks, floppy disks, back-up tapes), or any other electronic data such as voice mail. As you know, your failure to comply with this notice can result in sanctions being imposed by the court for spoliation of evidence or potential evidence.

[PLAINTIFF OR DEFENDANT] demands 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 [OTHER PARTIES] and their 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 certain admissible evidence, information subject to disclosure rules, information responsive to discovery, or information that will lead to the discovery of admissible evidence, 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, text messages, instant messaging);
- Online Content (*e.g.*, social media posts and messages, tweets, website content);
- 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 all of these sources of ESI, even if you do not anticipate producing such ESI.

This 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. 12/1/15)* [INSERT APPLICABLE STATE COURT RULE HERE AS WELL]], 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 [Plaintiff's Complaint];
2. [ADD ALLEGATIONS IN CASE]
3. 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. **In addition, where any files have already been deleted, such deleted files which are reasonably recoverable must be immediately undeleted.**

**System Sequestration and 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,

stenography or the like). As an appropriate and cost effective preservation step, we suggest removing ESI systems, media, and devices from service and properly sequestering and protecting them. 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.

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 [START DATE] to [END DATE], 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 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.

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 email 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.

**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.

Thank you.

Very truly yours,

[SIGNATURE BLOCK]

## APPENDIX D

**Litigation Hold Letter to Your Own Clients:**

**PRIVILEGED AND CONFIDENTIAL ATTORNEY WORK PRODUCT**

[DATE]

[CLIENT]
[ADDRESS]

Re: [SUBJECT LITIGATION]

To _____:

This letter addresses an issue of great importance. The purpose of this letter is to ensure that no evidence or potential evidence relating to your dispute with_____ is lost, altered, or destroyed. The law requires that once litigation begins or is foreseeable, all potential parties must take reasonable steps to preserve all evidence, even if that means holding documents well beyond the minimum periods otherwise established by law or private record-retention policies. The destruction, loss, or significant alteration of evidence can cause a party to lose its claims and defenses, and can even subject that party to civil and criminal penalties. To assist you in satisfying your obligations, it is recommended you take the following five steps to ensure that all potential evidence, including electronic data, is preserved.

**First**, you should determine who will take the lead in preserving all information potentially relevant to this matter. That person must ensure that the following steps are taken in their entirety, and that no steps are accidentally skipped because of a presumption that it is another's responsibility. This person should also keep a log of the steps taken to preserve information.

**Second**, you should immediately contact both your current and former employees and agents who might possess relevant documents or electronic information related to this matter and ensure that they understand the importance of preserving all potentially relevant evidence. You are encouraged to have them contact me directly at [YOUR TELEPHONE NUMBER] if they need further explanation of their duty to preserve information.

**Third**, you should develop a strategy for preserving all electronic data in your possession, including consulting an information technology specialist if necessary. (We would be happy to recommend a specialist that can safely preserve all such electronic data.) As we discussed, you are required to preserve all relevant and potentially relevant electronic data, including but not limited to: digital communications (e-mails, text messages, social media posts and messages, online content); electronic documents (such as documents created using Microsoft Word, Excel, PowerPoint, Access and the like); data generated by calendaring, task management, and Personal

Information Management (PIM) software (such as Microsoft Outlook or Lotus Notes); data created with the use of Personal Data Assistants, Blackberries, iPhone/iPad, Android and similar devices; all data created with the use of document management software (Hummingbird, DocsOpen, Worldox, etc.); all data created with the use of paper and electronic mail logging and routing software; all Internet and Web-browser-generated history files, caches, and "cookies" files; all electronic activity logs; and employee personal e-mail accounts. Your duty to preserve all potentially relevant data extends to information contained on business and personal computers of you and your agents and employees.

**Fourth**, if you automatically dispose of or recycle digital or paper files, digital back-up tapes, optical diskettes, or other storage media (whether or not pursuant to a document retention policy), we strongly recommend suspending such programs for the pendency of this dispute. If you do not know if any such processes are in place with respect to electronic media in your network or other electronic system, you should immediately contact your IT department or specialist to determine whether any such policies are in place.

**Fifth**, if your document retention policy previously resulted in the destruction of electronically stored information that can still be reasonably recovered, please recover this information immediately. If it is possible to recover information for a significant period of time, please contact me to discuss the relevant period of time for recovery.

In taking these steps, we recommend that you err on the side of preservation. Further, if anyone affiliated with [OPPOSING PARTY] or their legal representatives, [OPPOSING COUNSEL], speaks to you about this lawsuit, do not answer any questions or provide any information. Instead, inform them you are represented by Kercsmar & Feltus PLLC and contact me immediately.

If you have any questions regarding this letter or the gathering of evidence for this dispute, please do not hesitate to contact me directly at [CONTACT NUMBER AND EMAIL ADDRESS].

Sincerely,

[SIGNATURE BLOCK]