

**KELLETT & BARTHLOW PLLC**  
KAREN L. KELLETT  
THEODORE O. BARTHLOW, III (“THAD”)  
CAITLYN N. WELLS  
MEGAN F. CLONTZ  
O. MAX GARDNER III, *Of Counsel*



11300 N. CENTRAL EXPRESSWAY, SUITE 301  
DALLAS, TEXAS 75243  
TEL. 214.696.9000  
FAX 214.696.9001

Date

*Via electronic mail and  
U.S. Certified Mail, Return Receipt Requested*

\_\_\_\_\_  
Servicer's RESPA Address

*Re: CASE NUMBER*

Dear \_\_\_\_\_,

I write as counsel for \_\_\_\_\_ (hereinafter "Debtor") to inform you of your clients' obligation to preserve documents, tangible things, and electronically stored information that are potentially relevant to the issues in this case.

As used in this letter, the terms you and your refer to each of the named Creditor, and their predecessors, successors, parents, subsidiaries, divisions and affiliates and their respective officers, directors, agents, attorneys, accounts, employees, partners, and other persons occupying similar positions of performing any functions on their behalf.

Much of the information that is subject to disclosure or likely to be responsive to discovery in this case will be 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. The term Electronically Stored Information (hereinafter "ESI") should be afforded the broadest possible meaning and includes (by way of example and not as an exclusive list) potentially relevant information electronically, magnetically, optically or otherwise stored as:

- digital communications (for example email, voicemail, and instant messaging)
- email service stores (for example lotus domino.nsf or Microsoft exchange.edb)
- word processed documents (for example Word or WordPerfect files and all drafts thereof)
- spreadsheets and tables
- accounting application data
- imaging and facsimile files
- scan recording of any conversations with the Debtor

- databases (for example Access, Oracle, SQL Server data)
- Contact and relationship data management (for example Outlook, Ask or Interaction)
- Calendar and diary application data
- online access data (for example temporary internet files, history files and cookies)
- presentations (for example PowerPoint and Corel presentations)
- network access and server activity logs relating to information exchanged between defendants and by defendants with third parties
- project management application data
- backup and archival files

Debtor hereby demands that you preserve both accessible and inaccessible ESI. That demand is reasonable and necessary. Pursuant to the Federal Rules of Civil Procedure you must identify all sources of ESI you decline to produce and demonstrate why such sources are not reasonably accessible. For good cause shown, the court may order production of ESI even if it is not reasonably accessible. Accordingly, you must preserve ESI that you deem inaccessible so as not to preempt the court's authority.

***Preservation requires immediate intervention***

You must act immediately to preserve potentially relevant ESI, including, without limitation, information and the earlier of a created or last modified date for ESI concerning the alleged debt account from the inception of the loan through the date of this demand. Adequate preservation of ESI requires more than simply refraining from efforts to destroy or dispose of such evidence. You must immediately intervene to prevent loss due to routine operations or malfeasance and employ proper techniques and protocols to preserve ESI. Booting a drive, examining its contents or running any application may irretrievably alter the evidence contained therein and constitute spoliation of evidence.

***Preservation requires action***

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 that litigation hold. You are further directed to immediately identify and modify or suspend features of your information systems and devices, which, in routine operation, operate to cause the loss of potentially relevant ESI. Examples of such features and operations that could result in spoliation include:

- purging the contents of email repositories by age, capacity or any other criteria
- using data or media wiping, disposal, erasure of encryption utilities or devices
- overriding erasing, destroying or discarding backup media
- reassigning, re-imaging or depositing of systems, servers, devices or media
- running antivirus or other programs affecting wholesale metadata alteration
- releasing or purging online storage repositories

- using metadata stripper utilities
- disabling server, packet or local instant messaging login
- executing drive or file defragmentation or compression programs

You should also determine if any home or portable systems used by officers, board members, or employees 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 smart phone, PDA, 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 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.

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

### **Guard against deletion**

You should anticipate that your officers, employees, or others may seek to hide, destroy or alter ESI. This is not a concern that is unique to you or your companies. Rather it is simply conduct that occurs with such regularity that any custodian of ESI and their counsel must anticipate and guard against its occurrence. You are directed to preserve complete backup tape sets (including differentials and incrementals) containing emails and ESI for any person involved in the handling of the Debtors' account, including the enforcement or preservation of any alleged rights under the loan documents from the loan's inception through the present. You should also take affirmative steps to prevent anyone with access to your data, systems or archives from seeking to modify, destroy, or hide ESI.

### **System sequestration or forensic sound imaging**

As an appropriate and cost-effective means of preservation you should remove from service and securely sequester the systems, media, and devices housing potentially relevant ESI of any lawyer or collection agency acting on your behalf that has taken action with respect to Debtor, whether in his bankruptcy case or thereafter. In the event that you deem it impractical to sequester those systems, we believe that the breadth of preservation required, coupled with the modest number of

Date

---

Page 4

systems implicated, dictates that forensically sound imaging of the systems identified above 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 imposes a significant threat of spoliation and data loss. Be advised that a conventional copy, backup or ghosting of a hard drive does not produce a forensically sound image because it only captures active, unlocked data files and fails to preserve forensically significant data existing in, for example, unallocated clusters and slack space.

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

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, dates of creation, and last modification or access. Metadata may be overwritten or corrupted by careless handling or improper preservation, including by moving, copying, or examining the contents of files.

As hard copies do not preserve electronic search ability 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 the forms.

We desire to work with you to agree upon an acceptable protocol for forensically sound preservation and can supply a suitable protocol. If you promptly disclose the preservation protocol you intend to employ, perhaps we can now identify any points of disagreement and resolve them.

I am 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 of production of evidence to which we are entitled, that failure would constitute spoliation of evidence.

Please confirm no later than \_\_\_\_\_ 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.

Very truly yours,

Date

---

Page 5

KELLETT & BARTHOLOW PLLC

Theodore O. Bartholow, III (“Thad”)  
*Attorney at Law*