TO NON-CLIENT PARTY/WITNESS OR NON-PARTY

DATE: _____

TO:

RE: Preservation Letter

Dear _____:

Please be advised that _____ ("____") believes electronically stored information to be an important and irreplaceable source of discovery and/or evidence in the above-referenced matter. The lawsuit requires preservation of all information from your clients' computer systems, removable electronic media, and other locations. This includes, but is not limited to, email and other electronic communication, word processing documents, spreadsheets, databases, calendars, telephone logs, contact manager information, Internet usage files, and network access information.

_____ should also preserve the following platforms in the possession of the Defendant or a third party under the control of _____ (such as an employee or outside vendor under contract): databases, networks, computer systems, including legacy systems (hardware and software), servers, archives, backup or disaster recovery systems, tapes, discs, drives, cartridges and other storage media, laptops, personal computers, internet data, personal digital assistants, handheld wireless devices, mobile telephones, paging devices, and audio systems (including voicemail).

All of the information contained in the letter should be preserved for the following dates and time periods: _____ to present.

PRESERVATION OBLIGATIONS

The laws and rules prohibiting destruction of evidence apply to electronically stored information in the same manner that they apply to other evidence. Due to its format, electronic information is easily deleted, modified or corrupted. Accordingly, _____ must take every reasonable step to preserve this information until the final resolution of this matter.

This includes, but is not limited to, an obligation to:

- Discontinue all data destruction and backup tape recycling policies;

- Preserve and not dispose of relevant hardware unless an exact replica of the file (a mirror image) is made;

- Preserve and not destroy passwords, decryption procedures (and accompany software), network access codes, ID names, manuals, tutorials, written instructions, decompression or reconstruction software;

- Maintain all other pertinent information and tools needed to access, review, and reconstruct necessary to access, view, and/or reconstruct all requested or potentially relevant electronic data.

DESCRIPTION OF DATA SOUGHT

This lawsuit requires preservation of all information in _____ computer systems, removable electronic media and other locations relating to _____, hereafter ("_____"). This includes, but is not limited to, email and other electronic communication, word processing documents, spreadsheets, databases, calendars, telephone logs, contact manager information, Internet usage files, and network access information.

Electronic Files. You have an obligation to preserve all digital or analog electronic files in electronic format, regardless of whether hard copies of the information exist. This includes preserving:

A. Active data (i.e., data immediately and easily accessible on the client's systems today);

B. Archived data (i.e., data residing on backup tapes or other storage media);

C. Deleted data (i.e., data that has been deleted from a computer hard drive but is recoverable through computer forensic techniques); and

D. Legacy data (i.e., data created on old or obsolete hardware or software).

E. _____ must preserve active, archived and legacy data including but not limited to:

1. Word-processed files, including drafts and revisions;

2. Spreadsheets, including drafts and revisions;

3. Databases;

4. CAD (computer-aided design) files, including drafts and revisions;

5. Presentation data or slide shows produced by presentation software (such as Microsoft PowerPoint);

6. Graphs, charts and other data produced by project management software (such as Microsoft Project);

7. Animations, images, audio, video and audiovisual recordings, MP3 players, and voicemail files.

8. Data generated by calendaring, task management and personal information management (PIM) software (such as Microsoft Outlook or Lotus Notes);

9. Data created with the use of personal data assistants (PDAs), such as PalmPilot, HP Jornada; Cassiopeia or other Windows CE-based or Pocket PC devices;

10. Data created with the use of document management software; and

11. Data created with the use of paper and electronic mail logging and routing software.

F. _____must preserve media used by _____ computers including but not limited to:

1. Magnetic, optical or other storage media, including the hard drives or floppy disks used by [Plaintiffs/Defendants/Third Party] computers;

2. Backup media (i.e., other hard drives, backup tapes, floppies, Jaz cartridges, CDROMs) and the software necessary to reconstruct the data contained on the media; and

3. Archived media (you should retain a mirror image copy of any media no longer in service but used during the relevant time period).

Hardware. _____has an obligation to preserve all electronic processing systems, even if they are replaced. This includes computer servers, stand-alone personal computers, hard drives, laptops, PDAs, and other electronic processing devices. _____ should retain copies of any hardware no longer in service but used during the relevant time period.

Emails. You have an obligation to preserve all potentially relevant internal and external emails that were sent or received. Email must be preserved in electronic format, regardless of whether hard copies of the information exist.

Internet Web Activity. You have an obligation to preserve all records of Internet and Web-browser generated files in electronic format, regardless of whether hard copies of the information exist. This includes Internet and Web-browser-generated history files, caches and "cookies" files stored on backup media or generated by an individual employed at _____.

Activity Logs. _____ must preserve all hard copy or electronic logs documenting computer use by _____.

Supporting Information. _____ must preserve all supporting information relating to the requested electronic data and/or media including:

A. Codebooks, keys, data dictionaries, diagrams, handbooks, or other supporting documents that aid in reading or interpreting database, media, email, hardware, software, or activity log information.

Information for Employees. _____ should preserve all data that contains the information described below for all employees involved in this JOB/PROJECT/LITIGATION:

A. Name(s) & Job Title(s);

B. Basic employee information, including name, date of birth, social security number, employee identification number, race, date hired (or re-hired), and educational background;

C. Employment performance evaluations or reviews;

D. All information, including W-2 forms, relating to compensation (including salary, bonuses, merit increases, stock options or other forms of compensation);

E. For each position held by the employee during the relevant time period, list the job title/position, salary level, function or description, location, division, department, subsidiary, time in position, and job status (covered or not covered), and whether the employee was full-time, part-time or temporary;

F. Any disciplinary action or employment contract violations; and

G. If the individual is a former employee, list the data of departure and reason for leaving.

DESCRIPTION OF DOCUMENTS AND MEDIA THAT SHOULD BE PRESERVED

Data Preservation. _____ should immediately preserve all data and information about the data (i.e., backup activity logs and document retention policies) relating to documents maintained in the ordinary course of business. This includes, but is not limited to, the information listed below.

A. Email and any relevant metadata, including message contents, header information, and email system logs that was sent or received by or is in the possession of the following parties and/or contains information about _____;

B. All active and deleted copies of any word processing files, spreadsheets, PowerPoint presentations, or other documents that are in the possession of _____ or anyone under _____ control and may be relevant to _____;

C. Databases and any information about the databases that are in the possession of _____ and may be relevant to _____;

D. All paper and/or electronic logs of computer system and network activity that pertain to electronic data storage that are in the possession of _____ and may be relevant to the _____;

E. All active and deleted copies of any electronic calendars or scheduling programs, including programs maintained on PDAs, that are in the possession of _____ and may be relevant to the _____; and

F. All active, archived, legacy, and deleted copies of any other electronic data that are in the possession of _____ and may be relevant to the _____.

DATA STORAGE DEVICES

Online Data Storage. If _____ uses online storage and/or direct access storage devices, they must immediately cease modifying or deleting any electronic data unless a computer forensic expert makes a mirror image of the electronic file, follows proper preservation protocols for assuring the accuracy of the file (i.e., chain of custody), and makes the file available for litigation.

Offline Data Storage. Offline data storage includes, but is not limited to, backup and archival media, floppy diskettes, magnetic, magneto-optical, and/or optical tapes and cartridges, DVDs, CDROMs, and other removable media. _____ should immediately suspend all activity that might result in destruction or modification of all of the data stored on any offline media. This includes overwriting, recycling or erasing all or part of the media. This request includes, but is not limited to, media used to store data from personal computers, laptops, mainframe computers, and servers.

Data Storage Device Replacement. If _____ replace(s) any electronic data storage devices, it may not dispose of the storage devices.

Preservation of Storage Devices. _____ may not modify, delete or otherwise alter (i.e., by data compression, disk de-fragmentation, or optimization routines) any electronic data unless a computer

forensic expert makes a mirror image of the electronic file, follows proper preservation protocols for assuring the accuracy of the file (i.e., chain of custody), and makes the file available for litigation. The expert must make a mirror image of active files, restored versions of deleted files, and restored versions of deleted file fragments, hidden files, and directory listings. This includes, but is not limited to, preserving electronic data (stored on online or offline storage devices) that came from the following hardware or software applications:

1. Fixed drives on stand-alone personal computers or laptops;

2. Network servers and workstations; and

3. Software application programs and utilities.

PRESERVATION COMPLIANCE

Activity Log. In order to show preservation compliance, _____ must maintain a log, documenting all alterations or deletions made to any electronic data storage device or any electronic data processing system. The log should include changes and deletions made by supervisors, employees, contractors, vendors, or any other third parties.

Mirror Images. _____ must secure a mirror image copy (a bit-by-bit copy of a hard drive that ensures the computer system is not altered during the imaging process) of all electronic data contained on the personal computers and/or laptops of the individuals listed below. The mirror image should include active files, deleted files, deleted file fragments, hidden files, directories, and any other data contained on the computer. _____ must also collect and store any offline or online storage devices that contain data from any electronic processing devices for the individuals listed below.

Chain of Custody. For each piece of media that _____ preserves, _____ must document a complete chain of custody. A proper chain of custody will ensure that no material changes, alterations or modifications were made while the evidence was handled. Chain of custody documentation must indicate where the media has been, whose possession it has been in, and the reason for that possession.

Electronic Data Created After This Letter. For any electronic data created after this letter or for any electronic processing systems used after this letter, _____ must take the proper steps to avoid destroying potentially relevant evidence. This includes following the above preservation protocols.

****

COMPLIANCE WITH _____ PRESERVATION OBLIGATIONS INCLUDES FORWARDING A COPY OF THIS LETTER TO ALL INDIVIDUALS OR ORGANIZATIONS THAT ARE RESPONSIBLE FOR ANY OF THE ITEMS REFERRED TO IN THIS LETTER.

IF THIS CORRESPONDENCE IS IN ANY RESPECT UNCLEAR, PLEASE CONTACT ME IMMEDIATELY.

Sincerely,