KROLL ONTRACK®

E-Discovery Sample Forms & Pleadings

- Rule 16 Pre-Trial Conference for Electronic Discovery: Questions to Ask
- Sample Preservation Letter to Client
- Sample Preservation Letter to Opponent or Third Party
- Sample Proposed Request for Production of Documents and Things
- Sample Proposed Order Appointing Third Party Neutral Expert
- Sample Fed.R.Civ.P.30(b)(6) Deposition Notice
- Sample Interrogatories
- Sample Non-Waiver and Confidentiality Agreement
- Sample Custodian Interview Sheet
- Sample Onsite Detail Gathering Questions

For more information on electronic discovery, paper discovery, and computer forensics, contact us at 800 347 6105.

KROLL ONTRACK®

RULE 16 PRE-TRIAL CONFERENCE FOR ELECTRONIC DISCOVERY: QUESTIONS TO ASK

I. The FRCP mandates meet and confer conferences relating to electronically stored information: Why have an electronic discovery pre-trial conference?

- To better understand opposing party's technical landscape
- To clarify the scope of document requests
- To resolve any production format disagreements which may reduce liability and costs later
- To reduce waste and reproduction of documents
- To pre-empt the negative impact of inadvertent production of confidential or privileged documents

II. When should electronic discovery pre-trial conferences occur?

- When either party has used or is likely to use a computer or any other type of electronic equipment with the capability to create or store any type of electronic information which is relevant to the suit
- When the suit involves any type of Internet or e-commerce-type activity

III. What should counsel discuss?

- *Preservation of Electronic Evidence*
  i. Have the parties implemented litigation hold policies or taken steps to preserve electronic data when they reasonably expected litigation to occur?
  ii. Do the parties have data deletion protocols written into their computer systems? How often do they run? Are the deleted records archived on back-up tapes?
  iii. Are the parties aware of the location and format of potential electronic evidence?
  iv. Are depositions of each party's retention coordinator necessary?

- *Scope of Discovery*
  i. Who is most likely the custodian of relevant electronic material?
  ii. How far back in time should the party produce electronic data?
  iii. For whom should the party produce electronic data that is related to that person?
    1. I.e., certain employees, agents, etc.?
  iv. What type of computer systems or electronic equipment capable of electronic data storage does each party have?
  v. Should the production extend into backup tapes or archive records of all computer activity?
  vi. Should it be limited by the type of computer device?
    1. I.e. should laptops, hard drives or other items such as BlackBerries or cell phones be produced for examination?
  vii. Should a party produce the physical electronic device even though data may have been deleted by the producing party since the requesting party may employ a computer forensic specialist to recover the deleted data?
  viii. Should search terms be employed to limit responsive documents?
  ix. Should SPAM or virus filters be applied to e-mails and attachments?

RULE 16 PRE-TRIAL CONFERENCE FOR ELECTRONIC DISCOVERY: QUESTIONS TO ASK (cont.)

x. Should the parties agree upon a neutral third-party or ask the court to appoint a Special Master to oversee the discovery process?

- *Privileged or Confidential Documents*
  i. Is it likely the electronic data may contain privileged or confidential information?
     1. I.e., trade secrets, licenses, copyrights, attorney-client communications, etc.
  ii. Do the parties want to waive privileges?
  iii. Do the parties want a "clawback agreement" implemented for the inadvertent production of confidential documents?
  iv. Do the parties want to allow for a "quick peek" of potentially confidential documents?
  v. Are Protective Orders or Confidentiality Agreements necessary?
  vi. What should happen should trial preparation material become inadvertently disclosed?

- *Chain of Custody Issues*
  i. Is either party going to hire an outside electronic discovery service provider? How will the service provider handle chain of custody?
  ii. If the documents will be handled internally how will chain of custody be handled?

- *Costs*
  i. Who should bear the costs of the production?

- *Timeliness*
  i. What is a reasonable time to search a party's entire electronic database, review and organize the relevant documents?
  ii. Should the normal time limits as provided by Fed. R. Civ. P. 26 be expanded when data with limited accessibility is involved?

- *Production Format*
  i. Should all documents be produced in a native file format or as TIFF images?
  ii. Will a litigation support load file be required?
  iii. Should the parties produce data with the metadata attached or hidden? Which metadata fields?
  iv. Should production be on read-only media such as CD-ROMs?

KROLL ONTRACK®

SAMPLE PRESERVATION LETTER – TO CLIENT

[Date]

_____
_____
_____

RE: [Case Name] - Data Preservation

Dear _____ :

Please be advised that the Office of General Counsel assistance believes electronically stored information to be an important and irreplaceable source of discovery and/or evidence in [description of event, transaction, business unit, product, etc.]. The lawsuit requires preservation of all information from [Corporation's] computer systems, removable electronic media and other locations relating to [description of event, transaction, business unit, product, etc.]. 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.

[Corporation] should also preserve the following platforms in the possession of the [Corporation] or a third party under the control of the [Corporation] (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).

Employees must take every reasonable step to preserve this information until further notice from the Office of General Counsel. *Failure to do so could result in extreme penalties against [Corporation].*

All of the information contained in the letter should be preserved for the following dates and time periods: [List dates and times].

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, [Corporation] 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 from [Corporation's] computer systems, removable electronic media and other locations relating to [description of event, transaction, business unit, product, etc.]. 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.

I. **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. [Corporation] 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. [Corporation] must preserve media used by [Corporation]computers including but not limited to:
    1. Magnetic, optical or other storage media, including the hard drives or floppy disks used by [Corporation] computers;

SAMPLE PRESERVATION LETTER – TO CLIENT (cont.)

2. Backup media (i.e., other hard drives, backup tapes, floppies, Jaz cartridges, CD-ROMs) 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 following time periods):
    a) [List times here]

II. Hardware. [Corporation] 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. [Corporation] should retain copies of any hardware no longer in service but used during the following time periods:

A. [List times here]

III. 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.

IV. 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 [Corporation].

V. Activity Logs. [Corporation] must preserve all hard copy or electronic logs documenting computer use by [Relevant Computer Users].

VI. Supporting Information. [Corporation] 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.

VII. Information for Employees. [Corporation] should preserve all data that contains the information described below for the following employees:

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 and/or other forms of compensation);

E. For each position held by the employee during [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.

VIII. Other Relevant Information

A. Documents relating to computer systems, programs, software, hardware, materials, tools or information that [Corporation] uses or used to track, monitor or prevent discriminatory employment practices.

B. From [time period] all documents that relate to any software or hardware computer changes affecting your Human Resources database.

DESCRIPTION OF DOCUMENTS AND MEDIA THAT SHOULD BE PRESERVED

I. Data Preservation. [Corporation] 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 for the employees listed below. 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 the following subjects:
   1. Parties:
      a) [Name(s) & Job Title(s)]
   2. Subject Matters:
      a) [List topics here]

B. All active and deleted copies of any word processing files, spreadsheets, PowerPoint presentations, or other documents that are in the possession of the following parties and/or contain information about the following subjects:
   1. Parties:
      a) [Name(s) & Job Title(s)]
   2. Subject Matters:
      a) [List topics here]

C. Databases and any information about the databases that are in the possession of the following parties and/or contain information about the following subjects:

SAMPLE PRESERVATION LETTER – TO CLIENT (cont.)

1. Parties:
    a) [Name(s) & Job Title(s)]
2. Subject Matters:
    a) [List topics here]

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 the following parties and/or contain information about the following subjects:
    1. Parties:
        a) [Name(s) & Job Title(s)]
    2. Subject Matters:
        a) [List topics here]

E. All active and deleted copies of any electronic calendars or scheduling programs, including programs maintained on PDAs, that are in the possession of the following parties and/or contain information about the following subjects:
    1. Parties:
        a) [Name(s) & Job Title(s)]
    2. Subject Matters:
        a) [List topics here]

F. All active, archived, legacy, and deleted copies of any other electronic data that are in the possession of the following parties and/or contain information about the following subjects:
    1. Parties:
        a) [Name(s) & Job Title(s)]
    2. Subject Matters:
        a) [List topics here]

SAMPLE PRESERVATION LETTER – TO CLIENT (cont.)

II. Data Storage Devices

A. *Online Data Storage.* If [Corporation] 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.

B. *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. [Corporation] 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.

C. *Data Storage Device Replacement.* If [Corporation] replaces any electronic data storage devices, [Corporation] may not dispose of the storage devices.

D. *Preservation of Storage Devices.* [Corporation] 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

I. Activity Log. In order to show preservation compliance, [Corporation] 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. [Corporation] 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

SAMPLE PRESERVATION LETTER – TO CLIENT (cont.)

contained on the computer. [Corporation] must also collect and store any offline or online storage devices that contain data from any electronic processing devices for the individuals listed below.

A. [Name(s) & Job Title(s)]

II. **Chain of Custody.** For each piece of media that [Corporation] preserve(s), [Corporation] 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.

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

****

Compliance with [Corporation] 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 call me immediately.

Sincerely,

John E. Doe

KROLL ONTRACK®

SAMPLE PRESERVATION LETTER – TO OPPONENT OR THIRD PARTY

[Date]

_____
_____
_____

RE: [Case Name] - Data Preservation

Dear _____ :

Please be advised that [Plaintiffs/Defendants] believe electronically stored information to be an important and irreplaceable source of discovery and/or evidence in [description of event, transaction, business unit, product, etc.]. The lawsuit requires preservation of all information from [Plaintiffs/Defendants/Third Party] 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.

[Plaintiffs/Defendants/Third Party] should also preserve the following platforms in the possession of the [Plaintiffs/Defendants/Third Party] or a third party under the control of the [Plaintiffs/Defendants/Third Party] (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: [dates and times].

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, [Plaintiffs/Defendants/Third Party] 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;

SAMPLE PRESERVATION LETTER – TO OPPONENT OR THIRD PARTY (cont.)

- 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 from [Plaintiffs/Defendants/Third Party] computer systems, removable electronic media and other locations relating to [description of event, transaction, business unit, product, etc.]. 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.

IX. 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. [Plaintiffs/Defendants/Third Party] 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. [Plaintiffs/Defendants/Third Party] must preserve media used by [Plaintiffs/Defendants/Third Party] 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, CD-ROMs) and the software necessary to reconstruct the data contained on the media; and

SAMPLE PRESERVATION LETTER – TO OPPONENT OR THIRD PARTY (cont.)

3. Archived media (you should retain a mirror image copy of any media no longer in service but used during the following time periods):
    a) [List times here]

X. Hardware. [Plaintiffs/Defendants/Third Party] [have/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. [Plaintiffs/Defendants/Third Party] should retain copies of any hardware no longer in service but used during the following time periods:

A. [List times here]

XI. 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.

XII. 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 [Organization].

XIII. Activity Logs. [Plaintiffs/Defendants/Third Party] must preserve all hard copy or electronic logs documenting computer use by [Plaintiffs/Defendants/Third Party].

XIV. Supporting Information. [Plaintiffs/Defendants/Third Party] 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.

XV. Information for Employees. [Plaintiffs/Defendants/Third Party] should preserve all data that contains the information described below for the following employees:

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 [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.

XVI. Other Relevant Information

A. Documents relating to computer systems, programs, software, hardware, materials, tools or information that [Plaintiffs/Defendants/Third Party] uses or used to track, monitor or prevent discriminatory employment practices.

B. From [time period] all documents that relate to any software or hardware computer changes affecting your Human Resources database.

DESCRIPTION OF DOCUMENTS AND MEDIA THAT SHOULD BE PRESERVED

III. Data Preservation. [Plaintiffs/Defendants/Third Party] 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 for the employees listed below. 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 the following subjects:
   1. Parties:
      a) [Name(s) & Job Title(s)]
   2. Subject Matters:
      a) [List topics here]

B. All active and deleted copies of any word processing files, spreadsheets, PowerPoint presentations, or other documents that are in the possession of the following parties and/or contain information about the following subjects:
   1. Parties:
      a) [Name(s) & Job Title(s)]
   2. Subject Matters:
      a) [List topics here]

C. Databases and any information about the databases that are in the possession of the following parties and/or contain information about the following subjects:
   1. Parties:
      a) [Name(s) & Job Title(s)]
   2. Subject Matters:
      a) [List topics here]

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 the following parties and/or contain information about the following subjects:
   1. Parties:
      a) [Name(s) & Job Title(s)]
   2. Subject Matters:
      a) [List topics here]

E. All active and deleted copies of any electronic calendars or scheduling programs, including programs maintained on PDAs, that are in the possession of the following parties and/or contain information about the following subjects:
   1. Parties:
      a) [Name(s) & Job Title(s)]
   2. Subject Matters:
      a) [List topics here]

F. All active, archived, legacy, and deleted copies of any other electronic data that are in the possession of the following parties and/or contain information about the following subjects:
   1. Parties:
      a) [Name(s) & Job Title(s)]
   2. Subject Matters:
      a) [List topics here]

IV. Data Storage Devices

A. *Online Data Storage.* If [Plaintiffs/Defendants/Third Party] use(s) 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.

B. *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. [Plaintiffs/Defendants/Third Party] 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.

C. *Data Storage Device Replacement.* If [Plaintiffs/Defendants/Third Party] replace(s) any electronic data storage devices, [Plaintiffs/Defendants/Third Party] may not dispose of the storage devices.

D. *Preservation of Storage Devices.* [Plaintiffs/Defendants/Third Party] 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

IV. Activity Log. In order to show preservation compliance, [Plaintiffs/Defendants/Third Party] 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.

V. Mirror Images. [Plaintiffs/Defendants/Third Party] 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. [Plaintiffs/Defendants/Third Party] must also collect and store any offline or online storage devices that contain data from any electronic processing devices for the individuals listed below.

A. [Name(s) & Job Title(s)]

VI. Chain of Custody. For each piece of media that [Plaintiffs/Defendants/Third Party] preserve(s), [Plaintiffs/Defendants/Third Party] 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.

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

****

Compliance with [Plaintiffs/Defendants/Third Party] 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 call me immediately.

Sincerely,

John E. Doe

KROLL ONTRACK®

SAMPLE PROPOSED REQUEST FOR PRODUCTION OF DOCUMENTS AND THINGS

UNITED STATES DISTRICT COURT
DISTRICT OF [jurisdiction]

Mr. Plaintiff P. Plaintiff Plaintiff, v. OF DOCUMENTS Mrs. Defendant D. Defendant Defendant.	Court File No.: REQUESTS FOR PRODUCTION

PLAINTIFFS' REQUEST FOR PRODUCTION OF DOCUMENTS AND THINGS

Pursuant to Rules 26 and 34 of the Federal Rules of Civil Procedure ("FRCP") Plaintiffs, by counsel, request Defendants to produce the documents specified below, within thirty (30) days of service, to [counsel's name and address], or at such other time and place, or in such other manner, as may be mutually agreed upon by the parties. Defendants' production of documents shall be in accordance with the Instructions and Definitions set forth below and Fed.R.Civ.P. 34.

INSTRUCTIONS AND DEFINITIONS

(a) Whenever reference is made to a person, it includes any and all of such person's principals, employees, agents, attorneys, consultants and other representatives.

(b) When production of any document in Plaintiffs' possession is requested, such request includes documents subject to the Plaintiffs' possession, custody or control. In the event that Defendant is able to provide only part of the document(s) called for in any particular Request for Production, provide all document(s) that Defendants are able to provide and state the reason, if any, for the inability to provide the remainder.

(c) "Document(s)" means all materials within the full scope of Fed.R.Civ.P. 34 including but not limited to: all writings and recordings, including the originals and all non-identical copies, whether different from the original by reason of any notation made on such copies or otherwise (including but without limitation to, email and attachments, correspondence, memoranda, notes, diaries, minutes, statistics, letters, telegrams, minutes, contracts, reports, studies, checks, statements, tags, labels, invoices, brochures, periodicals, telegrams, receipts, returns, summaries, pamphlets, books, interoffice and intraoffice communications, offers, notations of any sort of conversations, working papers, applications, permits, file wrappers, indices,

SAMPLE PROPOSED REQUEST FOR PRODUCTION OF DOCUMENTS AND THINGS (cont.)

telephone calls, meetings or printouts, teletypes, telefax, invoices, worksheets, and all drafts, alterations, modifications, changes and amendments of any of the foregoing), graphic or aural representations of any kind (including without limitation, photographs, charts, microfiche, microfilm, videotape, recordings, motion pictures, plans, drawings, surveys), and electronic, mechanical, magnetic, optical or electric records or representations of any kind (including without limitation, computer files and programs, tapes, cassettes, discs, recordings), including metadata.

(d) If any document is withheld from production under a claim of privilege or other exemption from discovery, state the title and nature of the document, and furnish a list signed by the attorney of record giving the following information with respect to each document withheld:

(i) the name and title of the author and/or sender and the name and title of the recipient;

(ii) the date of the document's origination;

(iii) the name of each person or persons (other than stenographic or clerical assistants) participating in the preparation of the document);

(iv) the name and position, if any, of each person to whom the contents of the documents have been communicated by copy, exhibition, reading or substantial summarization;

(v) a statement of the specific basis on which privilege is claimed and whether or not the subject matter or the contents of the document is limited to legal advice or information provided for the purpose of securing legal advice; and

(vi) the identity and position, if any, of the person or persons supplying the attorney signing the list with the information requested in subparagraphs above.

(e) "Relate(s) to," "related to" or "relating to" means to refer to, reflect, concern, pertain to or in any manner be connected with the matter discussed.

(f) Every Request for Production herein shall be deemed a continuing Request for Production, and Defendant is to supplement its answers promptly if and when Defendant obtains responsive documents which add to or are in any way inconsistent with Defendant's initial production.

(g) These discovery requests are not intended to be duplicative. All requests should be responded to fully and to the extent not covered by other requests. If there are documents that are responsive to more than one request, please note and produce each such document first in response to the request that is more specifically directed to the subject matter of the particular document.

(h) Any word written in the singular herein shall be construed as plural or vice versa when necessary to facilitate the response to any request.

(i) "And" as well as "or" shall be construed disjunctively or conjunctively as necessary in order to bring within the scope of the request all responses which otherwise might be construed to be outside its scope.

KROLL ONTRACK®

SAMPLE PROPOSED REQUEST FOR PRODUCTION OF DOCUMENTS AND THINGS (cont.)

DOCUMENT REQUESTS

1. All documents with reference to or written policies, procedures and guidelines related to Defendant's computers, computer systems, electronic data and electronic media including, but not limited to, the following:

   a. Backup tape rotation schedules;

   b. Electronic data retention, preservation and destruction schedules;

   c. Employee use policies of company computers, data, and other technology;

   d. File naming conventions and standards;

   e. Password, encryption and other security protocols;

   f. Diskette, CD, DVD, and other removable media labeling standards;

   g. Email storage conventions (i.e., limitations on mailbox sizes/storage locations, schedule and logs for storage, etc.);

   h. Electronic media deployment, allocation and maintenance procedures for new employees, current employees or departed employees;

   i. Software and hardware upgrades (including patches) for [relevant time period] (who and what organization conducted such upgrades); and

   j. Personal or home computer usage for work-related activities.

2. Organization charts for all Information Technology or Information Services departments or divisions from [relevant time period].

3. Backup tapes containing email and other electronic data related to this action from [relevant time period].

4. Exact copies (i.e., bit-by-bit mirror image copies) of all hard drives on the desktop computers, laptop computers, notebook computers, personal digital assistant computers, servers, and other electronic media related to this action from [relevant time period].

5. Exact copies of all relevant disks, CDs, DVDs and other removable media related to this action from [relevant time period].

KROLL ONTRACK®

SAMPLE PROPOSED REQUEST FOR PRODUCTION OF DOCUMENTS AND THINGS (cont.)

6. For each interrogatory set forth in Plaintiffs' First Interrogatories, produce all documents which Defendant referred to, relied upon, consulted or used in any way in answering such interrogatory.

7. All documents that contain or otherwise relate to the facts or information that Defendants contend refute, in any way, the allegations contained in the Complaint in this action.

8. All reports, including drafts, submitted by any expert witness or potential expert witness retained or consulted by any Defendant with respect to the issues raised in this case.

Date:

[LAW FIRM NAME]

_____

[ATTORNEY NAME & ID]

[ADDRESS]

[PHONE]

KROLL ONTRACK®

SAMPLE PROPOSED ORDER APPOINTING THIRD PARTY NEUTRAL EXPERT

UNITED STATES DISTRICT COURT
DISTRICT OF [jurisdiction]

Mr. Plaintiff P. Plaintiff, Plaintiff, v. Mrs. Defendant D. Defendant Defendant.	Court File No.: PROPOSED ORDER

Before this Court is the parties' joint motion to appoint Kroll Ontrack, Inc. ("Kroll Ontrack") as an officer of the Court to conduct certain computer and other electronic media discovery sought by Plaintiff. Accordingly, IT IS HEREBY ORDERED that Kroll Ontrack is appointed an officer of the Court to conduct certain computer and other electronic media discovery in this case. IT IS FURTHER ORDERED that:

1. Kroll Ontrack will inspect the hard drives used during [enter circumstances here] on the personal computers of [enter name] for the business of [enter corporation name here] or its predecessors. Kroll Ontrack shall perform specific electronic discovery tasks agreed to by the parties (and set forth in the protocol at Appendix A). The terms of Appendix A may be changed by written consent of the parties.
2. As an officer of the Court, Kroll Ontrack's inspection of the hard drives will not waive any applicable privilege or other doctrine or principal assuring the confidentiality of the information on those hard drives. Kroll Ontrack will maintain all information in the strictest confidence. No information learned by Kroll Ontrack shall be disclosed except

pursuant to the terms of this Order, other direction of the Court, or as business or legally necessary to complete the electronic discovery protocol.

3. Party representatives present at the mirror imaging shall be present only to observe. The mirror image shall be made at a location to be selected by counsel for Defendants. The computer personnel nominated by Defendants' counsel shall have the right, but are not required, to access the hard drive after Kroll Ontrack makes its mirror image for the purpose of making additional mirror images. Once Kroll Ontrack has completed making its mirror image, the hard drive may be returned to normal use or otherwise disposed of.
4. Kroll Ontrack shall have the right to shield from direct observation any proprietary procedures or processes used during the mirror image backups or its subsequent search of the mirror image backup for responsive information. If requested by any party, Kroll Ontrack shall make a representative of the company reasonably available for deposition or trial testimony to testify concerning its inspection and findings.
5. Defendants' counsel shall only be obligated to turn over files or other information generated by Kroll Ontrack that are non-privileged, responsive to Plaintiffs' discovery requests, and relevant to this action.
6. Within such time as the parties reasonably agree, after receiving the electronic data, records, files or other information from Kroll Ontrack, Defendants' counsel shall review the information for privilege and designation under the protective order and produce to Plaintiffs all non-privileged, responsive documents or other agreed-upon information generated by Kroll Ontrack. The parties shall make reasonable efforts to limit the extent of data produced by Kroll Ontrack for review by Defendants' counsel through methods such as modifying key words or other techniques that Kroll Ontrack suggests. Defendants shall also provide Plaintiffs with a privilege log sufficient to allow Plaintiffs to challenge any claim of privilege by Defendants.

SAMPLE PROPOSED ORDER APPOINTING THIRD PARTY NEUTRAL EXPERT (cont.)

7. Within [enter number of days], the protocol for communications between Kroll Ontrack and any of the parties shall be established and reasonably agreed upon by the parties.
8. Plaintiffs and Defendants shall bear the costs of Kroll Ontrack's work pursuant to protocol at Appendix A.
9. Within [enter number of days], the format for data output shall be agreed upon by the parties pursuant to protocol at Appendix A.

Dated:

_____
_____

The Honorable [JUDGE]
UNITED STATES DISTRICT
JUDGE

SAMPLE PROPOSED ORDER APPOINTING THIRD PARTY NEUTRAL EXPERT (cont.)

Appendix A

1. Create a list of all original media/equipment. This list acts as a log of all pertinent hardware and serial numbers. Each piece of media will be assigned a Kroll Ontrack media identification number.

2. Create a full mirror-image or bit-stream copy all hard drives in the targeted computer (as opposed to only the active files). Computer personnel nominated by Defendants' counsel will bring the computer to the location where Kroll Ontrack shall make the mirror image copy. This location shall be chosen by Defendants' counsel.

3. Conduct keyword searches on the active files of the hard drive using an agreed upon list of keywords. Produce a file listing of the files that contain the keyword hits.

4. ***OPTIONAL PARAGRAPH IN THE EVENT COMPUTER FORENSIC SERVICES ARE NEEDED.*** Extract whole files and all available remnants of unallocated, slack, or system data with files that contain keyword hits. Deleted data should be reassembled into as much of its original, active state as possible. Kroll Ontrack will produce any resulting data in the most technically practical format.

5. Kroll Ontrack shall produce the resultant data according to agreement of the parties. Output options are limited to industry standard outputs including: native format, litigation support database, online review repository, or printed paper.

6. Fees shall be apportioned as follows: [enter cost allocation agreement here].

7. The party noticing a deposition of any Kroll Ontrack representative or seeking his or her testimony at trial shall pay all costs and fees associated with such deposition or testimony, including the cost of preparing any expert report prepared in connection with that deposition or testimony.

KROLL ONTRACK®

SAMPLE FED.R.CIV.P. 30(b)(6) DEPOSITION NOTICE

UNITED STATES DISTRICT COURT
DISTRICT OF [Jurisdiction]

_____,	Plaintiff,	Court File No.:
v.		NOTICE OF TAKING
DEPOSITION		PURSUANT TO FED.R CIV P.
30(b)(6)		
_____,	Defendant.	

PLEASE TAKE NOTICE that [Plaintiff/Defendant/Corporation] take(s) the deposition, before a qualified notary public by oral examination, of [Plaintiff/Defendant/Corporation] on [date/time], commencing at [location]. The deposition will continue until adjournment.

Pursuant to Federal Rule of Civil Procedure 30(b)(6), [Plaintiff/Defendant] corporate designee(s) shall be prepared to testify regarding the following subjects, all with respect to [Plaintiff's/Defendant's] information technology systems:

1) Number, types, and locations of computers currently in use and no longer in use;
2) Past and present operating system and application software, including dates of use;
3) Name and version of network operating system currently in use and no longer in use but relevant to the subject matter of the action;
4) File-naming and location-saving conventions;
5) Disk or tape labeling conventions;
6) Backup and archival disk or tape inventories or schedules;
7) Most likely locations of electronic records relevant to the subject matter of the action;
8) Backup rotation schedules and archiving procedures, including any backup programs in use at any relevant
time;
9) Electronic records management policies and procedures;

SAMPLE FED.R.CIV.P. 30(b)(6) DEPOSITION NOTICE (cont.)

10) Corporate policies regarding employee use of company computers and data;

11) Identities of all current and former personnel who have or had access to network administration, backup, archiving, or other system operations during any relevant time period.

[Date]: _____ [LAW FIRM NAME]

_____

[ATTORNEY NAME & ID]

[ADDRESS]

[PHONE]

KROLL ONTRACK®

SAMPLE INTERROGATORIES

UNITED STATES DISTRICT COURT
DISTRICT OF [Jurisdiction]

_____,	Plaintiff,	Court File No.:
v.		FIRST SET OF
INTERROGATORIES		TO PLAINTIFF
_____,	Defendant.	

I. Definitions. The definitions below will apply to the interrogatories requested in this document.

A. Application: An application is a collection of one or more related software programs that enable a user to enter, store, view, modify or extract information from files or databases. The term is commonly used in place of "program," or "software." Applications may include word processors, Internet browsing tools and spreadsheets.

B. Backup: To create a copy of data as a precaution against the loss or damage of the original data. Most users backup some of their files, and many computer networks utilize automatic backup software to make regular copies of some or all of the data on the network. Some backup systems use digital audio tape (DAT) as a storage medium. Backup Data is information that is not presently in use by an organization and is routinely stored separately upon portable media, to free up space and permit data recovery in the event of disaster.

C. Deleted Data: Deleted Data is data that, in the past, existed on the computer as live data and which has been deleted by the computer system or end-user activity. Deleted data remains on storage media in whole or in part until it is overwritten by ongoing usage or "wiped" with a software program specifically designed to remove deleted data. Even after the data itself has been wiped, directory entries, pointers, or other metadata relating to the deleted data may remain on the computer.

D. Document: The term "document" encompasses all discoverable information within the scope of Fed. R. Civ. P. 34(a), including "all writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained." Accordingly, both paper-based documents and electronically stored information-including, but not limited to, emails, attachments, databases, word documents, spreadsheets and graphic files-are covered by this definition.

SAMPLE INTERROGATORIES (cont.)

E. Hard Drive: The primary storage unit on PCs, consisting of one or more magnetic media platters on which digital data can be written and erased magnetically.

F. Mirror Image: Used in computer forensic investigations and some electronic discovery investigations, a mirror image is a bit-by-bit copy of a computer hard drive that ensures the operating system is not altered during the forensic examination.

G. Network: A group of computers or devices that is connected together for the exchange of data and sharing of resources.

H. Operating system (OS): The software that the rest of the software depends on to make the computer functional. On most PCs this is Windows or the Macintosh OS. Unix and Linux are other operating systems often found in scientific and technical environments.

I. Spoliation: Spoliation is the destruction of records which may be relevant to ongoing or anticipated litigation, government investigations or audits. Courts differ in their interpretation of the level of intent required before sanctions may be warranted.

J. Software: Coded instructions (programs) that make a computer do useful work.

II. Documents and Data.

A. *Individuals/organizations responsible.* Identify and attach copies of all company organizational and policy information including:
   1. Organizational charts;
   2. A list of the names, titles, contact information, and job description/duties for all individuals (or organizations) responsible for maintaining electronic processing systems, networks, servers, and data security measures; and
   3. A list of the names, titles, contact information, and job description/duties for all individuals employed in the following departments (or their equivalents) for [Plaintiffs/Defendants/Third Party]:
      a) Information Technology;
      b) Information Services;
      c) Incident Response Teams;
      d) Data Recovery Units; and
      e) Computer Forensic or Audit/Investigation Teams.

B. *Relevant Products/Services.* Identify and attach copies of all documents related to (including marketing, selling, leasing, sharing or giving to another party) the computer system, programs, software, hardware, materials, tools or information that [Plaintiffs/Defendants/Third Party] uses or has used in relation to the sale or use of [Product/Service]. This includes all electronic data and necessary instructions for accessing such data relating to:
   1. The pricing of [Product/Service] in the United States and internationally;
   2. Customer invoices for [Product/Service], including the customer names/addresses, purchase volume, prices, discounts, transportation charges and production information;

SAMPLE INTERROGATORIES (cont.)

3. Email sent or received by [Plaintiffs/Defendants/Third Party] to customers relating to [Product/Service];
4. Accounting records relating to [Product/Service], including work-in-progress reports, billing records, vendor invoices, time and material records, cost completion reports for each of [Plaintiffs/Defendants/Third Party] customers;
5. Construction and development information relating to web pages offering sale of [Product/Service] to the public;
6. Internal reports, sales reports, customer backlog reports, supplier backlog reports and operation reports related to [Product/Service];
7. Financial reporting information on a monthly and annual basis including profit and loss statements, branch costs, contribution margins and corporate overhead relating to [Product/Service];
8. Budgeting, projection and forecasting information relating to [Product/Service]; and
9. Sales booked, gross profit dollars and percentage for the sales booked, net sales shipped, and gross and net profit dollars and percentages for [Product/Service].

C. *Networks.* As to each computer network, identify the following:
1. Brand and version number of the network operating system currently or previously in use (include dates of all upgrades);
2. Quantity and configuration of all network servers and workstations;
3. Person(s) (past and present, including dates) responsible for the ongoing operations, maintenance, expansion, archiving and upkeep of the network; and
4. Brand name and version number of all applications and other software residing on each network in use, including but not limited to electronic mail and applications.

D. *Hardware.* Identify and describe each computer that has been, or is currently, in use by [Plaintiffs/Defendants/Third Party] (including desktop computers, PDAs, portable, laptop and notebook computers, cell phones, etc.), including but not limited to the following:
1. Computer type, brand and model number;
2. Computers that have been re-formatted, had the operating system reinstalled or been overwritten and identify the date of each event;
3. The current location of each computer identified in your response to this interrogatory;
4. The brand and version of all software, including operating system, private and custom-developed applications, commercial applications and shareware for each computer identified;
5. The communications and connectivity for each computer, including but not limited to terminal-to-mainframe emulation, data download and/or upload capability to mainframe, and computer-to-computer connections via network, modem and/or direct connection; and
6. All computers that have been used to store, receive or generate data related to the subject matter of this litigation.

E. *Software.* Identify and describe all software programs that have been, or are currently, in use by [Plaintiffs/Defendants/Third Party] including, but not limited to, the following:
1. Titles;
2. Version Names and Numbers;
3. Manufacturers;

SAMPLE INTERROGATORIES (cont.)

4. Authors and contact information; and
5. Operating systems that the programs were installed on.

F. *Operating Systems.* Identify and describe all operating systems that have been, or are currently, in use by [Plaintiffs/Defendants/Third Party] including, but not limited to, operating systems installed during [time period] for the following individuals:
   1. [Name & Job Title]

G. *Email.* Identify all email systems in use, including but not limited to the following:
   1. All email software and versions presently and previously used by you and the dates of use;
   2. All hardware that has been used or is currently in use as a server for the email system including its name;
   3. The specific type of hardware that was used as terminals into the email system (including home PCs, laptops, desktops, cell phones, personal digital assistants, etc.) and its current location;
   4. The number of users there has been on each email system (delineate between past and current users);
   5. Whether the email is encrypted in any way and list passwords for all users;
   6. All users known to you who have generated email related to the subject matter of this litigation; and
   7. All email known to you (including creation date, recipient(s) and sender(s)) that relate to, reference or are relevant to the subject matter of this litigation.

H. *Internet Use.* Identify any Internet policies and procedures in use, including but not limited to the following:
   1. Any Internet Service Providers (ISP) that [Plaintiffs/Defendants/Third Party] has provided its employees and the method used to access the Internet;
   2. The names and titles for all individuals who had Internet access;
   3. Any Internet hardware or software documentation that is used to provide Internet access to the above individuals during [time period];
   4. Internet use/access manuals, policies and procedures, including limitations on Internet access and use; and
   5. All Internet-related data on the electronic processing systems used by [Plaintiffs/Defendants/Third Party] including, but not limited to, saved Web pages, lists of Web sites, URL addresses, Web browser software and settings, bookmarks, favorites, history lists, caches, and cookies.

I. *Other Electronic Data.* Identify any other electronic data in use, including but not limited to the following:
   1. Activity log files contained on [Plaintiffs/Defendants/Third Party] network and any equipment needed to access the log files;
   2. Manual and automatic records of hardware and equipment use and maintenance;
   3. The names of Internet newsgroups or chat croups that [Plaintiffs/Defendants/Third Party] subscribes to; include the name and title of the individuals subscribing to each group as well as any information necessary to access the groups, including passwords; and

4. Any portable devices that are not connected to [Plaintiffs/Defendants/Third Party] network and that are not backed up or archived.

J. *Data Transmission.* Describe in detail all inter-connectivity between the computer system at [opposing party] in [office location] and the computer system at [opposing party # 2] in [office location # 2] including a description of the following:
   1. All possible ways in which electronic data is shared between locations;
   2. The method of transmission;
   3. The type(s) of data transferred;
   4. The names and contact information of all individuals possessing the capability for such transfer, including list and names of authorized outside users of [opposing party's] electronic mail system; and
   5. The name and contact information of the individual responsible for supervising inter-connectivity.

K. *Data security measures.* List all user identification numbers and passwords necessary for accessing the electronic processing systems or software applications requested in this document. During the course of this litigation, you must supplement all security measures with updated information, if applicable. Include:
   1. Computer security policies;
   2. The name(s) and contact information of the individual(s) responsible for supervising security; and
   3. Information about each applications security settings, noting specifically who has administrative rights.

L. *Supporting information.* All codebooks, keys, data dictionaries, diagrams, handbooks, manuals or other documents used to interpret or read the information on any of the electronic media listed above.

III. Backup Protocols.

A. *Current Procedures.* As to data backups performed on all computer systems currently or previously in use, identify and describe the following:
   1. All procedures and devices used to back up the software and the data including, but not limited to, name(s) of backup software used, the frequency of the backup process, and type of tape backup drives, including name and version number, type of media (i.e. DLT, 4mm, 8mm, AIT). State the capacity (bytes) and total amount of information (gigabytes) stored on each tape;
   2. The tape or backup rotation, explain how backup data is maintained, and state whether the backups are full or incremental (attach a copy of all rotation schedules);
   3. Whether backup storage media is kept off-site or on-site. Include the location of such backup and a description of the process for archiving and retrieving on-site media;
   4. The name(s) and contact information for the individual(s) who conduct(s) the backup and the individual who supervises this process;
   5. A detailed list of all backup sets, regardless of the magnetic media on which they reside, showing current location, custodian, date of backup, a description of backup content and a full inventory of all archives,

SAMPLE INTERROGATORIES (cont.)

6. All extra-routine backups applicable for any servers identified in response to these Interrogatories, such as quarterly archival backup, yearly backup, etc., and identify the current location of any such backups, and
7. Any users who had backup systems in their PCs and describe the nature of the backup.

B. *Backup Tapes.* Identify and describe all backup tapes in your possession including:
   1. Types and number of tapes in your possession (such as DLT, AIT, Mammoth, 4mm, 8mm);
   2. Capacity (bytes) and total amount of information (gigabytes) stored on each tape; and
   3. All tapes that have been re-initialized or overwritten since commencement of this litigation and state the date of said occurrence.

IV. Spoliation of Electronic Evidence.

A. *Document Retention and Destruction Policies.* Identify and attach any and all versions of document/data retention or destruction policies used by [opposing party] and identify documents or classes of documents that were subject to scheduled destruction.
   1. Attach copies of document destruction inventories/logs/schedules containing documents relevant to this action.
   2. Attach a copy of any disaster recovery plan.
   3. Also state:
      a) The date the policy was implemented;
      b) The date, if any, of the suspension of this policy *in toto* or any aspect of said policy in response to this litigation;
      c) A description by topic, creation date, user or bytes of any and all data that has been deleted or in any way destroyed after the commencement of this litigation. State whether the deletion or destruction of any data pursuant to said data retention policy occurred through automation or by user action; and
      d) Whether any company-wide instruction regarding the suspension of the data retention/destruction policy occurred after or related to the commencement of this litigation. If so, identify the individual responsible for enforcing the suspension.

B. *Document Destruction.* Identify any data that has been deleted, physically destroyed, discarded, damaged (physically or logically), or overwritten, whether pursuant to a document retention or destruction policy or otherwise, since the commencement of this litigation. Specifically identify those documents that relate to or reference the subject matter of the above referenced litigation.

C. *Organizations or Individuals Responsible for Maintaining the Document Retention and Destruction Policies.* List the job title, description, business address, telephone number, and email address of any individuals or organizations that are/were responsible for creating, implementing or retaining any and all versions of your document retention or destruction policies.

SAMPLE INTERROGATORIES (cont.)

D. *Meetings or Documents Discussing Document/Data Destruction.* Identify with specificity any meetings or conversations referencing document spoliation in relation to this action.
   1. Identify and attach any and all related meeting minutes/notes from [time period here].
   2. List the job title, description, business address, telephone number, and email address of any individuals or organizations that are/were responsible for retaining the meeting minutes/notes.

E. *Data Wiping.* For any server, workstation, laptop, or home operating system that has been "wiped clean", defragmented, or reformatted such that you claim that the information on the hard drive is permanently destroyed, identify the following:
   1. The date on which each drive was wiped, reformatted, or defragmented;
   2. The method or program used (i.e., WipeDisk, WipeFile, BurnIt, Data Eraser, etc.).

F. *Data Recycling.* Identify the person(s) responsible for maintaining any schedule of redeployment or circulation of existing equipment and describe the system or process for redeployment.

DATED: _____

[LAW FIRM NAME]

_____

[ATTORNEY NAME & ID]

[ADDRESS]

[PHONE]

KROLL ONTRACK®

SAMPLE NON-WAIVER AND CONFIDENTIALITY AGREEMENT

NON-WAIVER AND CONFIDENTIALITY AGREEMENT ("Agreement")

WHEREAS, the parties have agreed to produce all documents deemed discoverable under the Federal Rules of Civil Procedure, including Electronically Stored Information ("ESI"), that are responsive to each other's discovery requests and not privileged or otherwise exempted from discovery under the Federal Rules of Evidence, Federal Rules of Civil Procedure or other applicable source of law;

WHEREAS, some of the ESI and other documents produced in this matter may contain attorney-client privileged communications or other information protected as "privileged" under the Federal Rules of Evidence ("Privileged Material") and not subject to discovery under the Federal Rules of Civil Procedure or the Federal Rules of Evidence ("Privileged Material");

WHEREAS, some of the produced ESI and other documents in this matter may contain protected attorney work-product material prepared or compiled in anticipation of litigation and not subject to discovery under the Federal Rules of Civil Procedure or the Federal Rules of Evidence ("Work-Product Material");

WHEREAS, the parties acknowledge that, despite each party's best efforts to conduct a thorough pre-production review of all ESI and other documents, some Work Product Material and Privileged Material ("Protected Material") may be inadvertently disclosed to the other party during the course of this litigation;

WHEREAS, the volume of potentially discoverable ESI may substantially increase the total volume of documents that will be produced by the parties, thereby exacerbating the risk of inadvertent disclosure of Protected Material;

WHEREAS, in the course of this litigation, the parties may —either inadvertently or knowingly— produce information that is of a confidential, private, personal, trade secret, or proprietary nature ("Sensitive Material");

WHEREAS, the undersigned parties desire to establish a mechanism to avoid waiver of privilege or any other applicable protective evidentiary doctrine as a result of the inadvertent disclosure of Protected Material; and (b) keep disclosed Protected Material and Sensitive Material confidential to the maximum extent possible;

IT IS HEREBY STIPULATED AND AGREED by the parties that the following clauses of this Agreement shall govern the disclosure of Protected Material and Sensitive Material in this action.

NON-WAIVER OF PRIVILEGE OR OTHER PROTECTIVE DOCTRINE BY INADVERTENT DISCLOSURE

1. The inadvertent disclosure of any document which is subject to a legitimate claim that the document should have been withheld from disclosure as Protected Material shall NOT waive any privilege or other applicable protective doctrine for that document or for the subject matter of the inadvertently disclosed document if the producing party, upon becoming aware of the disclosure, promptly requests its return and takes reasonable precautions to avoid such inadvertent disclosure.

2. Except in the event that the requesting party disputes the claim, any documents which the

SAMPLE NON-WAIVER AND CONFIDENTIALITY AGREEMENT (cont.)

producing party deems to contain inadvertently disclosed Protected Material shall be, upon written request, promptly returned to the producing party or destroyed at the producing party's option. This includes all copies, electronic or otherwise, of any such documents. In the event that the producing party requests destruction, the requesting party shall provide written certification of compliance within thirty (30) days of such written request. In the event that the requesting party disputes the producing party's claim as to the protected nature of the inadvertently disclosed material, a single set of copies may be sequestered and retained by and under the control of requesting party for the sole purpose of seeking court determination of the issue pursuant to Federal Rule of Civil Procedure 26(b)(5)(B).

3. Any such Protected Material inadvertently disclosed by the producing party to the requesting party pursuant to this Agreement, shall be and remain the property of the producing property.

4. To the extent there may be inconsistency between the aforementioned stipulations in this Agreement and Federal Rule of Civil Procedure 26(b)(5) and the accompanying Committee Note, Rule 26(b)(5)(B) and the Committee Note shall control.

Confidential Treatment of Sensitive Material

5. Any Protected Material or Sensitive Material disclosed in this litigation is to be considered confidential and proprietary to the producing party and the requesting party shall hold the same in confidence and shall not use any disclosed Protected Material or Sensitive Material other than for the purposes of this litigation. To that end, the parties shall limit the disclosure of all Protected Material and Sensitive Material only to those persons with a need to know the information for purposes of supporting their position in this litigation. Moreover, Protected Material and Sensitive Material will not be disclosed, published or otherwise revealed to any other party in this litigation except with the specific prior written authorization of the producing party.

6. If Protected Material or Sensitive Material is disclosed through inadvertence or otherwise to any person not authorized under this Agreement, the party causing such disclosure shall inform the person receiving the Protected Material or Sensitive Material that the information is covered by this Agreement, make its best efforts to retrieve the Protected Material or Sensitive Material, and promptly inform the producing party of the disclosure.

7. The requesting party shall have no confidentiality obligations with respect to any information which:
   a. is already known to the requesting party without restriction;
   b. is or becomes publicly known otherwise than by the requesting party's breach of this Agreement;
   c. is received by the requesting party without restriction from a third-party who is not under an obligation of confidentiality;
   d. is independently developed by the requesting party;
   e. is approved for release by written authorization of the producing party; or
   f. is disclosed by the requesting party pursuant to judicial action, provided that producing party is notified at the time such action is initiated.

8. Any Protected Material or Sensitive Material disclosed by the producing party to the requesting party pursuant to this Agreement shall be and remain the property of the producing property.

KROLL ONTRACK®

SAMPLE NON-WAIVER AND CONFIDENTIALITY AGREEMENT (cont.)

General Provisions

9. This Agreement terminates and supersedes all prior understandings or agreements on the subject matter hereof.

10. This Agreement shall be binding on the parties hereto when signed regardless of whether or when the court enters its Agreement thereon.

11. Nothing herein shall prevent any party from applying to the court for a modification of this Agreement should the moving party believe the Agreement, as originally agreed upon, is hampering its efforts to prepare for trial; or from applying to the court for further or additional protective Agreements; or from an Agreement between the parties to any modification of this Agreement, subject to the approval of the court.

12. This Agreement shall survive the final termination of this case regarding any retained documents or contents thereof.

13. The effective date of this Agreement shall be _____.

DATED: _____

LAW FIRM NAME

_____
ATTORNEY NAME, BAR #
ADDRESS
CITY, STATE
PHONE NUMBER

DATED: _____

LAW FIRM NAME

_____
ATTORNEY NAME, BAR #
ADDRESS
CITY, STATE
PHONE NUMBER

KROLL ONTRACK®

SAMPLE CUSTODIAN INTERVIEW SHEET

Name: _____

Title: _____

Department: _____

E-mail Questions	Yes	No
How long have you been located at this office? Where were you before you moved to this office? How long have you been with the company?		
Have you changed your e-mail configuration from company default?		
If yes, how have you changed it?		
Do you move messages to personal folders?		
Do you receive e-mail messages on a blackberry, PDA or other portable device?		
If yes, was this PDA/Portable device acquired through a Third Party? (Best Buys, etc.)		
Are you routing your mailbox so that you receive company emails on this Third Party device?		
Is this PDA/Portable device approved and set up by corporate IT?		
Have you moved messages to a CD or other storage media?		
Do you use web-based mail at home?		

If yes, do you open & reply to company related messages from your personal computer?		
If yes, who is your service provider?		
What percentage of the time do you think that you use this method to receive business emails?		
Do you open attachments from your personal computer?		
Have you ever saved those attachments to your home computer before sending them out?		
Do you attach to the network via VPN or other devices? Explain		
Do you ever print your e-mail and put it in subject or chronological folders?		
Do you ever download e-mails to removable media, ie USB drive, etc.		
Do you maintain your Archive folder locally? Where is it?		

Calendar Questions	Yes	No
Do you keep your calendar on outlook?		
Do you use a PDA?		
Do you use a paper-based calendar?		
Do you print pages from your electronic calendar and add notes or change meetings as the day progresses?		
If you use a printed page, what do you do with those pages?		

Documents

Question	Yes	No
Where do you store your documents such as MS Word and Excel?		
Do you use a network drive? What is the directory address?		

KROLL ONTRACK®

Do you use a personal shared drive on the server?		
If yes, what is the address?		
Do you use a department share to save data?		
If yes, please list the various directories.		
What type of documents do you often generate or receive?		
Word		
Excel		
Pictures		
Others		
Do you have any work-related documents on a personal computer?		

Interviewer:_____ **Date:**_____

Interviewee: _____**Date:** _____

KROLL ONTRACK®

SAMPLE ONSITE DETAIL GATHERING QUESTIONS

1. Identify all email systems in use, including but not limited to the following:

   (a.) List all email software and versions presently and previously used by you and the dates of use;
   (b) Identify all hardware that has been used or is currently in use as a server for the email system including its name;
   (c) Identify the specific type of hardware that was used as terminals into the email system (including home PCs, laptops, desktops, cell phones, personal digital assistants ["PDAs"], etc.) and its current location;
   (d) State how many users there have been on each email system (delineate between past and current users);
   (e) State whether the email is encrypted in any way and list passwords for all users;
   (f) Identify all users known to you who have generated email related to the subject matter of this litigation;
   (g) Identify all email known to you (including creation date, recipient(s) and sender) that relate to, reference or are relevant to the subject matter of this litigation.

2. Identify and describe each computer that has been, or is currently, in use by you or your employees (including desktop computers, PDAs, portable, laptop and notebook computers, cell phones, etc.), including but not limited to the following:

   (a) Computer type, brand and model number;
   (b) Computers that have been re-formatted, had the operating system reinstalled or been overwritten and identify the date of each event;
   (c) The current location of each computer identified in your response to this interrogatory;
   (d) The brand and version of all software, including operating system, private and custom-developed applications, commercial applications and shareware for each computer identified;
   (e) The communications and connectivity for each computer, including but not limited to terminal-to-mainframe emulation, data download and/or upload capability to mainframe, and computer-to-computer connections via network, modem and/or direct connection;
   (f) All computers that have been used to store, receive or generate data related to the subject matter of this litigation.

3. As to each computer network, identify the following:

   (a) Brand and version number of the network operating system currently or previously in use (include dates of all upgrades);
   (b) Quantity and configuration of all network servers and workstations;
   (c) Person(s) (past and present including dates) responsible for the ongoing operations, maintenance, expansion, archiving and upkeep of the network;
   (d) Brand name and version number of all applications and other software residing on each network in use, including but not limited to electronic mail and applications.

KROLL ONTRACK®

SAMPLE ONSITE DETAIL GATHERING QUESTIONS (cont.)

4. Describe in detail all inter-connectivity between the computer system at [opposing party] in [office location] and the computer system at [opposing party # 2] in [office location # 2] including a description of the following:

   (a) All possible ways in which electronic data is shared between locations;
   (b) The method of transmission;
   (c) The type(s) of data transferred;
   (d) The names of all individuals possessing the capability for such transfer, including list and names of authorized outside users of [opposing party's] electronic mail system.
   (e) The individual responsible for supervising inter-connectivity.

5. As to data backups performed on all computer systems currently or previously in use, identify the following:

   (a) All procedures and devices used to back up the software and the data, including but not limited to name(s) of backup software used, the frequency of the backup process, and type of tape backup drives, including name and version number, type of media (i.e. DLT, 4mm, 8mm, AIT). State the capacity (bytes) and total amount of information (gigabytes) stored on each tape;
   (b) Describe the tape or backup rotation and explain how backup data is maintained and state whether the backups are full or incremental (attach a copy of all rotation schedules);
   (c) State whether backup storage media is kept off-site or on-site. Include the location of such backup and a description of the process for archiving and retrieving on-site media;
   (d) The individual(s) who conducts the backup and the individual who supervises this process;
   (e) Provide a detailed list of all backup sets, regardless of the magnetic media on which they reside, showing current location, custodian, date of backup, a description of backup content and a full inventory of all archives.

6. Identify all extra-routine backups applicable for any servers identified in response to these interrogatories, such as quarterly archival backup, yearly backup, etc. and identify the current location of any such backups.

7. For any server, workstation, laptop, or home PC that has been "wiped clean", defragmented, or reformatted such that you claim that the information on the hard drive is permanently destroyed, identify the following:

   (a) The date on which each drive was wiped, reformatted, or defragmented;
   (b) The method or program used (e.g., WipeDisk, WipeFile, BurnIt, Data Eraser, etc.).

8. Identify and attach any and all versions of document/data retention policies used by [opposing party] and identify documents or classes of documents that were subject to scheduled destruction. Attach copies of document destruction inventories/logs/schedules containing documents relevant to this action. Attach a copy of any disaster recovery plan. Also state:

   (a) The date, if any, of the suspension of this policy *in toto* or any aspect of said policy in response to this litigation;
   (b) A description by topic, creation date, user or bytes of any and all data that has been deleted or in any way destroyed after the commencement of this litigation. State whether the deletion or destruction of any data pursuant to said data retention policy occurred through automation or by user action;
   (c) Whether any company-wide instruction regarding the suspension of said data retention/destruction policy occurred after or related to the commencement of this litigation and if so, identify the individual responsible for enforcing said suspension.

KROLL ONTRACK®

SAMPLE ONSITE DETAIL GATHERING QUESTIONS (cont.)

9. Identify any users who had backup systems in their PCs and describe the nature of the backup.

10. Identify the person(s) responsible for maintaining any schedule of redeployment or circulation of existing equipment and describe the system or process for redeployment.

11. Identify any data that has been deleted, physically destroyed, discarded, damaged (physically or logically), or overwritten, whether pursuant to a document retention policy or otherwise, since the commencement of this litigation. Specifically identify those documents that relate to or reference the subject matter of the above referenced litigation.

12. Identify any user who has downloaded any files in excess of ten (10) megabytes on any computer identified above since the commencement of this litigation.

13. Identify and describe all backup tapes in your possession including:
    (a) Types and number of tapes in your possession (such as DLT, AIT, Mammoth, 4mm, 8mm);
    (b) Capacity (bytes) and total amount of information (gigabytes) stored on each tape;
    (c) All tapes that have been re-initialized or overwritten since commencement of this litigation and state the date of said occurrence.