



14030 Thunderbolt Place, Suite 700, Chantilly, Virginia 20151 • 703.375.4340 • fax 703.375.4343 • www.corefacts.net

DISCOVERY IN THE DIGITAL AGE

DISCOVERY IN THE DIGITAL AGE

Presented by: CoreFacts, LLC

Definitions:

ELECTRONIC DISCOVERY: The production of original evidence in electronic form; such evidence is computer-generated and may exist on, among other locations, hard drives, backup tapes, personal digital assistants, shared (network) storage, CDs, Zip drives, Jaz drives, and floppy disks.

ELECTRONIC DOCUMENTS: Information created, stored, and/or utilized using computer technology, business applications, Internet applications (such as e-mail), peripheral and mobile devices, and computer-based record storage.

ACTIVE DATA: Information that resides on the user's hard drive and/or network server and is readily available and accessible to computer users through file manager programs.

BACKUP DATA: Information copied to a removable media, such as a tape, for the purpose of disaster recovery, such as a system failure; usually contains everything on a server or some other centralized storage medium or network; often in a compressed form.

FILE SLACK: partial data from an older file or files still residing on the hard drive that has been allocated to a newer file but not used up by this newer file.

FREE SPACE: space on hard drive (or other storage medium) that appears to contain no data because this space is unused or because data that had been intact and accessible at one time are now erased.

LEGACY DATA (Archival Data): Information stored on media that is not in a user-friendly format and difficult to access; can no longer be accepted or organized in a format that can be read using current software; may have to hire technician to write program to retrieve data.

METADATA (or Embedded Data): Data about data, consisting of information within the electronic version of a document that travels with the file and that may not be apparent in a printed version of the document or when viewed on the monitor, such as author, title, subject, size of file, editing history, distribution route of document.

MIRROR IMAGE (Bit Stream Image): Process of creating an exact duplicate of computer memory onto secure storage medium; includes all files, file slack, errors, and residual space.

RESIDUAL DATA: Deleted files and e-mail to which the reference has been removed from the directory listings and file allocation table, and therefore, may be overwritten with another file; usually recoverable until overwritten.

Basic Rules For Computer Forensics:

1. Do not alter original evidence.
2. Do not execute programs on a computer that contains discoverable electronic data (especially programs affecting the operating system).
3. Do not allow anyone who is not properly trained or authorized to interact with the computer; in other words, isolate and preserve the computer.
4. Always create a mirror image of a computer hard drive and work with the mirror image; never alter the original.
5. Document all investigative activities.

OVERVIEW

1. Four Points to Remember:

- a. Electronic documents are NOT the same as printed documents.
- b. Attorneys have a duty to preserve potentially relevant evidence (including evidence in electronic form) when they know or reasonably should know that litigation is likely.
- c. Attorney must deal with electronic data as soon as possible because this information can easily disappear.
- d. Appellate law on electronic discovery is undeveloped. Most decisions are trial-level decisions, and on some points these decisions vary widely.

2. Electronic discovery is an issue because most information is now in electronic form and often only in electronic form

- a. Ken Withers estimates 99% of all information generated in 1999 was in digital form.
- b. In *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 2002 U.S. Dist. LEXIS 488 (S.D.N.Y. 2002) the court cited authority that one-third of all electronic documents are never printed.

EVOLVING LEGAL DUTIES

1. General

- * Main point to understand – The rules have not changed regarding preservation and production of relevant evidence, only the nature and the volume of the evidence have.
- * F.R. Civ. Pro. 26 (a)(1)(B) provides for mandatory disclosure of data compilations (electronic documents) that the disclosing party may use to support its claims or defenses. Therefore, counsel will have to make important decisions about case strategy at an early stage in the litigation.

2. Take The Defensive – The Duty To Preserve

a. When To Preserve

- i. The most common statement is the duty to preserve commences when the party has notice that the information is potentially relevant or reasonably likely to be requested during discovery. *Applied Telematics, Inc v. Sprint Communications Co.*, 1996 U.S. Dist. LEXIS 14053 (E.D. Pa. 1996); *Thompson v. General Nutrition Co.*, 593 F.Supp. 1443 (C.D. Cal. 1984); see Civil Discovery Standards at IV, “Document Production,” ABA Section of Litigation (August 1999).
- ii. In *Turner v. Hudson Transit Lines*, 142 FRD 68 (S.D.N.Y. 1991), the court said the duty to preserve could arise *prior to the filing of the complaint* if a party is on notice of pending litigation. In *Lewy*

v. Remington Arms Co., 836 F.2d 1104 (8th Cir. 1988) the court said there is a duty to preserve where the information is likely to be relevant to *foreseeable* litigation.

- iii. In our view, the duty to preserve arises when counsel believes the attorney-work product privilege attaches. It may be difficult to assert the work product privilege if you are not taking steps to preserve digital data.

b. What Must Be Preserved

- i. Active files must be preserved.
- ii. Back-up tapes must no longer be overwritten. In *Applied Telematics, Inc. v. Sprint Communications Co.*, 1996 U.S. Dist. LEXIS 14053 (E.D.Pa. 1996) the court concluded that Sprint's normal backup and recycling of backup tapes should have been suspended during the litigation.
- iii. Residual data
 1. Deleted files are not necessarily gone forever. By hitting delete, the user simply tells the computer that the space is free to be overwritten. Although it is not apparent to the user, the data still resides until some or all of it is overwritten, and a forensic expert can often recover this information.
 - a. **CoreFacts case example: Our client was a large company that purchased a smaller company. The owner of the smaller company remained working with our client until his buy-out and then left to start a competitive venture. A review of the deleted files in his computer revealed that he had taken certain software packages from our client and solicited its employees. A review of the deleted space in current employees' computers also identified key evidence, including emails to the former owner sending him proprietary information and emails indicating they were doing work for the competitive venture while still employed by our client.**
 2. There is some argument that deleted data is in the party's possession or is the equivalent of documents already shredded or discarded in the dumpster. Documents that have been deleted are discoverable under R. 34. *Simon Property Group v. mySimon, Inc.*, 194 F.R.D. 639 (S.D. Ind. 2000), citing *Crown Life Insurance Co. v. Craig*, 995 F.2d 1376 (7th Cir. 1993). Similarly, citing *Anti-Monopoly, Inc. v. Hasbro, Inc.*, 1995 WL 649934 (S.D.N.Y. 1995), the N.Y. State Bar Association's Report concluded that a judge will rule that any electronic information, no matter how it is

generated, is a “document” within R. 34. “*Does Discovery of Electronic Information Require Amendment to The Federal Rules of Civil Procedure?*” Commercial & Federal Litigation Section, Committee on Federal Procedure, New York State Bar Assoc. Report (February 22, 2001).

However, in *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 2000 U.S. Dist. LEXIS 488 (S.D.N.Y. 2002), the court analogized deleted e-mail messages to hard copy documents that had been discarded in the trash and declined to compel defendant to retrieve them.

3. In cases involving misappropriation of trade secrets, it is particularly important to access and analyze the subject hard drive. Employees who steal proprietary information do so by using their computers during the last few months of their employment. They may send information to home e-mail accounts, create memos outlining new ventures, or download key files to floppy discs. Employees may think they are covering their tracks by deleting these incriminating activities prior to leaving. However, a forensic expert can recover some or all of this information, and companies should therefore preserve the hard drives of employees upon their departures.
 - a. **CoreFacts case example: We were hired to assist a law firm in their dispute with a former partner and several associates who set up a competing firm and took numerous clients. A CoreFacts expert made a mirror image of the defectors’ computers and found two key pieces of evidence. The first was a memo by one of the defectors outlining a plan to “use leverage” if the firm fought too hard. This leverage included public disclosure about firm members’ personal behavior (drinking, adultery) to “ruin marriages and lives.” The second was a memo entitled “game plan” that outlined what to steal, destroy and copy from the firm. As a result of our findings, a TRO/PI was granted quickly, and our client filed a RICO claim against the defectors.**
4. Because of the nature of electronic evidence, parties believe it is worth the gamble to attempt to hide what is on the hard drive from inspection, anticipating that by producing hard copy versions of the hard drive content the opponent will not pursue the matter. In some cases, the party will take a desperate step, such as wiping the hard drive clean. *TY, Inc. v. Le Clair*, 2000 WL 1015936 (N.D.Ill. 2000).

- a. **CoreFacts case example: In a software infringement suit, the plaintiff alleged that his former employer stole his computer programs. In discovery, the plaintiff provided paper copies of screen shots of the programs at issue that contained author, and time/date stamp metadata. These shots gave the impression the programs were created by the plaintiff before he joined the defendant company. CoreFacts assisted the defendant company in gaining a court order to access to plaintiff's hard drive where the files were allegedly stored. Our experts found that in the 24 hour period prior to the arranged pick-up, a formatting program been run, 13.5 gigs of new software had been installed, and a defrag program had been run twice. Our report indicated that the plaintiff had purposely destroyed evidence, and the plaintiff settled the day before we were supposed to testify.**
 - b. **CoreFacts case example: A biomedical company suspected its head scientist stole proprietary information when he left to work for a start-up firm. Indeed, when we investigated the scientist's laptop on behalf of the company, we found evidence that processing methods and other intellectual property had been stolen. We also discovered that the scientist had installed a program intended to destroy data on the drive. Our findings lead to a favorable settlement.**
5. Even if residual data may not be required to be produced in every case, this type of electronic data is discoverable with a showing of deceptive conduct during discovery. *See Illinois Tool Works, Inc. v. Metro Mark Products, Ltd.*, 43 FS 2d 951 (ND. Ill. 1999).
 6. A party's admission that e-mail messages had been routinely deleted in the ordinary course of business after the lawsuit was filed was part of the basis for the court to permit Playboy to access the computer hard drive to attempt to recover the deleted e-mail messages. *Playboy Enterprises, Inc. v. Welles*, 60 F. Supp. 2d 1050 (S.D. Ca. 1999).

GENERAL RULE: if you think relevant evidence resides in free space or slack space, its best to preserve it.

- c. Failing to preserve electronic evidence may subject you to sanctions!
- i. Default Judgment: *Computer Associates International, Inc v. American Fundware, Inc.*, 133 F.R.D. 166 (D.Colo. 1990); *Thompson v. General Nutrition Co.*, 593 F.Supp. 1443 (C.D. Cal. 1984)
 - ii. Adverse Inference Instruction: *Shamis v. Ambassador Factors Corp.*, 34 F.Supp.2d 879 (S.D.N.Y. 1999); *Linnen v. A.H. Robins Co.*, 1999 Mass. Super. LEXIS 240 (Mass. Superior Ct., June 15, 1999); *Reingold v. Wet N' Wild Nevada, Inc.*, 944 P.2d 800 (Nev. 1997); *Shaefer v. RWP Group, Inc.*, 169 F.R.D. 19 (E.D.N.Y. 1996).
 - iii. Shifting of costs and/or payment of attorney's fees and expenses: *Trigon Insurance Co. v. United States*, 204 F.R.D. 277, 2001 U.S. Dist. LEXIS 18824 (E.D.Va. 2001); *GTFM, Inc. v. Wal-Mart*, 2000 U.S. Dist. LEXIS 3804 (S.D.N.Y. 2000); *Illinois Tool Works, Inc. v. Metro Mark Products, Ltd.*, 43 F.Supp.2d 951 (N.D.Ill. 1999).
- d. Avoiding Sanctions With a Records Retention Program
- i. Many businesses have established record management programs to reduce the potential liability for spoliation *See, e.g., Carlucci v. Piper Aircraft Corp.*, 102 F.R.D. 472 (S.D. Fla. 1984) (a bona fide, consistent and reasonable document retention policy may be a valid justification for failure to produce documents).
 - ii. However, these programs can create a risk of spoliation if they are improperly drafted or used improperly. Such a policy may be just as harmful as no policy at all. *See, e.g., In re Prudential Ins. Co. of America Sales Practices Litigation*, 169 F.R.D. 598 (D.N.J. 1997) (Prudential's haphazard and uncoordinated approach to document retention denied its opponents potential evidence to establish facts in dispute and was grounds for severe sanctions – a fine of \$1 million imposed on Prudential); *Reingold v. Wet N' Wild Nevada, Inc.*, 944 P.2d 800 (Nev. 1997) (court found records management policy did not account for applicable statute of limitations for events covered in the records and destruction of documents amounted to suppression of evidence, requiring adverse inference instruction).
 - iii. In *Lewy v. Remington Arms Co.*, 836 F.2d 1104 (8th Cir. 1988), the court established a standard to determine the reasonableness of a record management program. The trial court had instructed the jury that they could draw a negative inference from Remington's destruction of documents pursuant to their record retention policy. The 8th Circuit remanded for further consideration of the reasonableness of the record retention policy under four criteria. The 8th Circuit also concluded that some circumstances may compel the retention of certain documents notwithstanding a

general destruction policy, such as when a corporation knows or should have known that the documents would become material at some point in the future. It said a corporation may not blindly destroy documents pursuant to a stated policy and expect to be shielded from liability in all circumstances.

- e. How to preserve electronic evidence
 - i. Call your client and make a “reasonable inquiry” about the location of potentially relevant evidence. Be sure to ask the proper individual and to document the instructions given. Include some form of verification of the individual’s actual compliance with your advice. See *GTFM, Inc. v. Wal Mart*, 2000 US Dist LEXIS 3804 (S.D.N.Y. 2000)(one year after Wal Mart VP told counsel the company could not retrieve electronic documents, MIS employee stated otherwise; court granted plaintiff’s motion to conduct on-site inspection of computer system and for sanctions).
 - 1. Counsel should instruct client to preserve both hard copy and electronic version of the documents. *Thompson v. General Nutrition Co.*, 593 F.Supp. 1443 (C.D. Cal. 1984).
 - 2. Sanctions may be imposed even if the particular employee responsible for the records in question did not know to preserve the records. *National Association of Radiation Survivors v. Turnage*, 115 F.R.D. 543 (N.D.Cal. 1987).
 - ii. See Attachment 2 for sample matters to review with client.
 - iii. Mirror imaging is only way to preserve residual data. See e.g. *Gates Rubber Co. v. Bando Chem. Indus. Ltd.*, 167 FRD 90 (D. Colo. 1996). Gates was ordered to preserve computer records, but chose an unqualified computer technician, not a computer forensic expert, to copy the files. The procedure used by Gates’ expert overwrote about 8% of the hard drive before he even began to copy the documents. Court concluded that Gates should first have created a mirror image of the hard drive.
- f. Why Simply Preserving Printed Copies of Electronic Data is Not Sufficient.
 - i. Black letter law that electronic data is discoverable even if it is never reduced to printed form. See e.g. *Crown Life Ins. v. Craig*, 995 F. 2d 1376 (7th Cir. 1993). *Accord Rowe Entertainment, Inc. v. William Morris Agency*, 2002 U.S. Dist. LEXIS 488 (S.D.N.Y. 2002).
 - ii. The requesting party can obtain the data in computerized form even though it possesses the hard copy of the information. *Williams v. E.I. duPont Nemours & Co.*, 119 F.R.D. 648 (W.D. Kent. 1987). “[T]he rule is clear; production of information in ‘hard copy’ documentary form does not preclude a party from receiving that same information in computerized/electronic form.”

Anti-Monopoly, Inc. v. Hasbro, Inc., 1995 WL 649934 (S.D.N.Y. 1995).

- iii. It is also black letter law that the electronic files are different than paper documents. See Armstrong v. Executive Office of the President, 1 F.3d 1274 (D.D.C. 1993)(hard copy of e-mail was not the same as the electronic version as it did not contain directories, distribution list, acknowledgment of receipts, transmittal information.)
- iv. In sum, relying solely on information in paper form will mean that you are missing important information. Electronic discovery “could make or break a case.” Withers, Electronic Discovery: The Challenges and Opportunities of Electronic Evidence, Nat’l Workshop for Magistrate Judges, July 23-25, 2001.

3. How To Take The Offensive

- a. Send preservation of evidence letter – See Attachment 2.
- b. Conduct 30(b)(6) deposition at an early stage in discovery. These depositions should seek to identify how the opponent maintains its data and what hardware/software is necessary to access the information that may be covered under document request. See Attachment 3.
- c. Sample Interrogatories are provided in Attachment 4.
- d. Based on the responses, you may decide to seek a protective order, motion to compel, or sanctions. A sample motion to access the hard drive of a computer is provided in Attachment 5.

4. Controlling Costs

- a. Upon motion of counsel or upon the courts own initiative, F.R. Civ. P 26 (b)(2) (i)-(iii) can be used to limit unreasonable discovery requests. Counsel for defendants relied on this rule in opposing plaintiffs’ “sweeping” requests and seeking to shift the costs from defendants to plaintiffs in Rowe Entertainment, Inc. v. William Morris Agency, Inc., 2002 U.S. Dist. LEXIS. 488 (S.D.N.Y. 2002).
- b. It is unwise to use client’s in-house IT personnel because of independence issues, skills factor, etc. IT personnel are trained to provision services, not to conduct computer forensics or electronic data recovery.
- c. Can costs of electronic discovery be shifted?
 - i. The courts have treated the cost issue differently. There is no bright line rule.
 - ii. Some courts refuse to shift the costs because the responding party chose the technology that created the expense of production. See In re Brand Name Prescription Drugs Antitrust Litigation, 1995 WL 360526 (N.D. Ill. 1995); Daewoo Electronics v. US, C Intl Trade 1986; (“The normal and reasonable translation of electronic data into a form usable by the discovering party should be the

ordinary and foreseeable burden of a respondent in the absence of a showing of extraordinary hardship”); Linnen v. A.H. Robins Co., 1999 Mass. Super.LEXIS 240 (Superior Ct., June 15, 1999).

- iii. The foreseeable risk argument was rejected in Rowe Entertainment, Inc. v. William Morris Agency, Inc., 2002 U.S. Dist. LEXIS 488 (S.D.N.Y. 2002) and in McPeck v. Ashcroft, 202 F.R.D. 31, 2001 U.S. Dist. LEXIS 12061 (D.D.C. 2001). In Rowe, the court did not agree that the necessity for retrieving stored electronic data is an ordinary and foreseeable risk. In this court’s opinion, parties retain electronic data because the costs are nil and there is no compelling cost reason to discard such data. Moreover, data is not stored for retrieval purposes but is simply uploaded in its entirety onto a backup tape for disaster recovery purposes. In McPeck, the court noted that if the producing party has to pay for all restoration costs merely because it chose to use computers, the requesting party has no disincentive to demand anything less than all tapes. It therefore adopted a “marginal utility” approach – i.e., the more likely that a backup tape contains information that is relevant to a claim or defense, the fairer it is that the producing party pay.
- iv. Some courts use balancing approaches. See Rowe Entertainment, Inc. v. William Morris Agency, Inc., 2002 U.S. Dist. LEXIS 488 (S.D.N.Y. 2002); Bills v. Kennecott Corp., 108 F.R.D. 459 (D.Utah 1985).

d. Using Neutral Experts

- i. Several courts have recognized that permitting the computer forensic expert of one party to have unsupervised access to the hard drive of the opponent creates the risk of waiver of the attorney-client privilege, disclosure of trade secrets, and access to irrelevant information. To manage this concern, these courts have followed the protocol first developed in Playboy Enterprises, Inc. v. Welles, 60 F.Supp.2d 1050 (S.D.Cal. 1999); followed in Simon Property Group v. mySimon, Inc., 194 F.R.D. 639 (S.D.Ind. 2000); Northwest Airlines, Inc v. Local 2000, Int’l Brotherhood of Teamsters, C.A. No. 00-08 (D.Minn. 2000).
- ii. The Playboy “protocol” includes: court-appointed neutral expert; mirror image of hard drive; expert to recover deleted files and perform searches; potentially responsive files to be turned over initially to counsel for producing party; after review by counsel, relevant and non-privileged files are to be produced to counsel for requesting party; producing party pays for the neutral expert. Our sample engagement letter follows this protocol.
- iii. In Rowe Entertainment, Inc. v. William Morris Agency, Inc., 2002 U.S. Dist. LEXIS 488 (S.D.N.Y. 2002), the court chose another protocol. The principal difference involves the process of review

of potentially privileged e-mail messages of defendants. If defense counsel wanted to conduct the privilege review of the electronic documents prior to their production to plaintiffs' counsel, then defendants would bear the cost of that portion of the production. Otherwise, at plaintiffs' expense, plaintiffs' counsel (not the clients) would receive all documents, whether privileged or not; they would select the responsive documents; they would deliver to defense counsel hard copies of these documents; and defense counsel would object and assert privilege on the appropriate documents. The court decreed that defendants would not be waiving any privilege claim by agreeing to this protocol.

1. CoreFacts case example – Our expert was chosen to work as the parties' independent computer forensic expert in a trade secret matter. We conducted an investigation of the hard drive at issue and found that data had been purposefully deleted.

- e. How to Obtain a Price Quote From an Electronic Discovery Firm
- i. The following are some questions you should expect the provider of electronic data recovery services to ask before providing a quotation:
- What is the universe of electronic storage involved? For example, how many servers, workstations, back-up tapes are involved
 - What is the type of storage? For example, Windows based, Unix based, DLT, or DAT
 - What is the size of the storage? For example, number of gigabytes
 - What is needed from the storage? For example, e-mails, documents, database information, slack space, deleted files
 - What can be excluded from the scope of the production? For example, what dates, what individuals, and/or what directories or folders can be excluded?
 - What format is required for the production? For example, paper, native file format, common file format, remote access
 - Will metadata have to be preserved? If yes, what is counsel's definition of metadata?
 - What is the deadline for completion?
 - Where will the storage media be produced – on site or off site? If on site, will there be any restrictions on the time that the electronic data may be captured?
 - Will counsel require an expert to be involved in the production to provide an affidavit or testimony?
 - Is counsel concerned about chain of custody, data security, and/or confidentiality issues?

Deleted: in case

Deleted: is needed

- ii. Quotations may use a variety of price elements. Once a quotation has been received, counsel should analyze the price elements as follows:
- If the quote is for an hourly rate, does the quote provide a cap that will not be exceeded without prior authorization from counsel and does the hourly rate only apply to the time spent by the expert and not the processing time?
 - If the quote is per page, what pages are to be produced? How will pages be counted?
 - If the quote is per e-mail user, what is included?
 - If the quote is per file, what constitutes a file and is the price based on the files processed or only on the files produced?

ATTACHMENT 1

Suggested Steps for Counsel to Take At Earliest Possible Time

1. Take these steps at least as early as you would claim the protection of the attorney-work product privilege, preferably even earlier.
2. Learn about client's technology.
3. Identify and meet with your client's R. 30(b)(6) IT representative.
 - a. Go over this person's knowledge of client's computer systems, including hardware and major, company-approved software
 - b. Go over this person's knowledge of client's networking configurations and accessing of client's computer systems by 3rd parties
 - c. Go over this person's knowledge of employees' use while at their residences of computers for business purposes
 - d. Learn about the client's disaster recovery backup procedures, including where backup tapes are stored, how long, and legacy systems that may have been used
 - e. Advise this person about how backup procedures should be modified to prevent unintended spoliation
 - f. Identify a manager of client who has sufficient authority within client's organization to oversee the notification and compliance with preservation of electronic data/compilations until further notice – include verification and compliance with these instructions
4. Identify and meet with your client's R. 30(b)(6) records management representative.
 - a. Go over client's records management policy and ongoing procedures. Determine if this policy addresses electronic documents and placing a "legal hold," which suspends the destruction of documents, including electronic documents, when litigation is probable or underway.
 - b. Advise this person about suspending portion of record management procedures that entail deleting company records to prevent unintended spoliation.
 - c. Identify a manager of client who has sufficient authority within client's organization to oversee the notification and compliance with suspension of any destruction of records pursuant to the client's ongoing records

management program until further notice – include verification and compliance with these instructions

5. Review your discovery materials to ensure that the standard instructions and definitions address electronic compilations/data are clear, and up-to-date.
 - a. Modify these materials as appropriate for the instant litigation.

ATTACHMENT 2

Sample Letter Addressing Preservation of Evidence

Dear _____:

We represent _____ [Plaintiff/Defendant] in this matter.

As you know, Federal Rules of Civil Procedure 26(a)(1)(B) and 34 (a) and applicable case law provide that electronic documents are discoverable. The Federal Rules regarding destruction of evidence apply to electronic data in the same manner as the rules apply to other forms of evidence.

[Plaintiff(s)/Defendant(s)] consider electronic data to be an important and irreplaceable source for discovery and/or evidence. Today, over 90% of all information is generated in electronic form. Millions of transactions with legal significance take place daily using computer and/or electronic technology. We intend to submit discovery requests to access your client's computer network(s) and computer systems and to seek the production of documents in their electronic form. Access to the computer network(s) and computer systems as well as access to documents in their electronic form is critical because the paper form of text derived from an electronic file does not preserve the totality of information that is in the electronic file itself. Therefore, preservation and production of the paper text alone does not constitute the full preservation of evidence.

We request that a copy of this letter be provided promptly to the person(s) who are responsible for your client's computer network and computer systems and to the person(s) who are responsible for your client's record management program. Until the parties reach agreement for the protocols to discover electronic documents and this agreement is memorialized in an order of the court, we request that your client take the broadest view of their obligation under the Federal Rules to preserve relevant electronic documents and take the following steps to safeguard against the destruction of evidence.

Specifically, we request that your client preserve:

- a) All electronic mail and information about electronic mail (including message contents, header information and logs of electronic mail system usage) sent or received by [list names, job titles, or job responsibilities];
- b) All other electronic mail and information about electronic mail (including message contents, header information and logs of electronic mail system usage) about [describe the subject matter];
- c) All data bases (including all records and fields and structural information in such databases) containing any reference to and/or information about [describe the subject matter];
- d) All logs of activity on computer systems that may have been used to process or store electronic data containing information about [describe the subject matter];
- e) All word processing files and file fragments containing information about [describe the subject matter];
- f) All electronic data and file fragments created by application programs which process financial, accounting and billing information about [describe the subject matter];
- g) All electronic files and file fragments containing information from electronic calendars and scheduling programs regarding [describe the subject matter];
- h) All electronic data files and file fragments created or used by electronic spreadsheet programs where such data files contain information about [describe the subject matter]; and
- i) All other electronic data containing information about [describe the subject matter].

To minimize the risk of spoliation of relevant electronic documents, your client also:

Should not modify or delete any electronic data files that are maintained in on-line storage and/or direct access storage devices which exist as of the delivery of this letter and meet the criteria of ¶¶ (a) – (i), unless a true and correct copy of each such electronic data file has been made and steps have been taken to ensure that such copy will be preserved and accessible. (On-line storage and/or Direct Access storage)

Should stop any activity that may result in the loss of such electronic data meeting the criteria of ¶¶ (a) – (i) in electronic media used for off-line

storage, including magnetic tapes and cartridges and other media. This activity includes rotation, destruction, overwriting and/or erasure of such media in whole or in part. (Off-line Storage)

Should preserve any electronic data storage devices and/or media that may contain electronic data meeting the criteria of ¶¶ (a) – (i) which may be replaced due to failure and/or upgrade or for any other reason.

(Replacement of Data Storage Devices)

Should not alter or erase such electronic data meeting the criteria of ¶¶ 1(a) –(i) and should not perform any other procedures (such as data compression and disk de-fragmentation or optimization routines) which may impact such data on any stand-alone microcomputers and/or network workstations, unless a true and correct copy had been made of such active files and of completely restored versions of such deleted electronic files and file fragments and unless copies have been made of all directory listings (including hidden files) for all directories and subdirectories containing such files, and unless arrangements have been made to preserve copies. (Fixed Drives on Standalone Personal Computers and Network Workstations)

Should preserve copies of all application programs and utilities that may be used to process electronic data described in ¶¶ 1(a) – (i). (Programs and Utilities)

Should maintain an activity log that documents all modifications made to any electronic data processing system that may affect the system's capability to process any electronic data meeting the criteria described in ¶¶ (a) – (i). (Log of System Modifications)

Should to take the following steps immediately with respect to all personal computers used by [list personnel] and/or their secretaries or assistants. (Personal Computers)

- A true and correct copy should be made of all electronic data on fixed drivers attached to such personal computers relating [describe subject matter], including all active files and completely restored versions of all deleted electronic files and file fragments.
- Full directory listings (including hidden files) for all directories and subdirectories (including hidden directories) on such fixed drivers should be written.
- The copies and listings made should be preserved until this matter reaches its final resolution.

- All floppy diskettes, magnetic tapes and cartridges, and other media in connection with such computers prior to the date of delivery of this letter containing any electronic information relating in any manner to the matters in dispute should be collected and put into storage until this matter reaches its final resolution.

Should take whatever steps are appropriate to preserve relevant evidence created subsequent to this letter. (Evidence Created Subsequent to this Letter)

We appreciate your prompt attention to these matters. Please contact me if you have any questions.

ATTACHMENT 3

Sample Rule 30(b)(6) Deposition Questions

Counsel will have his/her own style for framing questions of the Rule 30(b)(6) deponent. Here are some suggested subject areas to address during the Rule 30(b)(6) deposition:

1. Qualifications and Organizational Structure:

- a. Education, training or experience of the deponent [particularly experience or training in handling and investigating computer evidence; IT personnel are trained to provision systems and lack training in forensics].
- b. Where in the organization does the deponent sit – to whom does the deponent report and who reports to the deponent.
- c. The company's use of consultants or outside vendors for maintenance and service of computer systems (hardware, software, and networks).
- d. The role/responsibility the deponent has (or will have) in responding to discovery requests seeking production of electronic documents, such as information created, stored, and/or utilized using computer technology.
- e. Steps taken by deponent to prepare for deposition, including document review.

2. Information about the party's systems:

- a. Duties of system administrators
- b. Use of passwords by users, sharing of passwords, access to passwords by system administrator(s)
- c. Details about hardware used by deponent's employer (may include model numbers and/or hard drive capacity)
- d. Networking of desktop computers
- e. Information about operating systems for network servers, including model versions

- f. Details about creating, storing and retrieving of back up tapes (hard drives, servers, e-mail system)
- g. Details about disaster recovery procedure (software is used to convert back up tapes into usable format)
- h. Details about facsimile machines used by deponent's employer and the procedures to use fax machines (e.g., fax logs, memory of fax machines)

3. Software and E-Mail:

- a. Details about application software used on desktops and laptops (including company standard software, such as Word, Excel, Power Point; length of time this software was company standard, what version)
- b. Details about company-approved/standards for personal digital assistants (e.g., hand-held devices such as Palm Pilot)
- c. Details about e-mail system(s) used by deponent's employer (retention period, use of files, deletion procedures)

4. Record Management and Document Preservation:

Formatted

- a. Notification and instructions about preservation of documents due to the lawsuit (who provided the notification, how was it communicated)
- b. Details of any deletion of documents since commencement of lawsuit or since deponent received notification about lawsuit or reasonable possibility of lawsuit
- c. Details about company's record management policy (when instituted, when electronic documents became part of this policy, who is responsible for ongoing management of this policy, provide copy during deposition)
- d. Determine if he/she has examined any computers since learning of this lawsuit; if yes, establish details about protocol IT person used

5. Alternative sources of electronic information:

- a. Identify any locations outside deponent's employer where electronic documents are regularly sent
- b. Names (and location, etc.) of persons who would have knowledge about 3rd party's computer systems

- c. Details about Internet site of employer (access by 3rd parties, content, who develops content, intervals for revision)
6. Backup Procedures:
- a. Details about company's backup procedures (including intervals, medium for backup, reuse of backup medium, location of backup)
 - b. Since filing of lawsuit, has any backup tape been reused or otherwise erased (details about this)
7. Production of electronic documents in other lawsuits:
- a. Details about electronic production in other lawsuits (what cases, what was produced, format of production)
 - b. Information about use of this electronic documentation in other litigation (at depositions, to support motions, at trial on merits)
8. Hardware:
- a. Details about disposal/recycling/sale of hardware (including what happens to hard drives)
9. Legacy Systems:

Details about software used for backup media or archived documentation (include information whether deponent retains legacy software and manuals)

ATTACHMENT 4

Sample Interrogatories

Formatted

System Archaeology

[There are many computer systems and network configurations. It may be useful to learn more about your opponent's electronic systems before engaging in the core part of electronic discovery. These interrogatories will assist in gaining an overall idea of the opposition's computer systems and network configurations. These sample interrogatories may be narrowed to focus on smaller departments or operating groups within a department. These interrogatories will also be useful during interviews or depositions of key witnesses associated with the opposition's computer systems.]

1. Describe in detail the layout of the computer system, including, but not limited to, the number and type of computers and the type(s) of operating system(s) and application software packages used. [You will want as much detail as you can obtain about connectivity, names and versions of software programs used for electronic mail, calendars, project management files, word processing, and database management.]
2. For each of the following individuals [insert names] provide a detailed description of their computer(s), including desktop computers, personal digital assistants, portable, laptop and notebook computers. If an individual uses a computer for business purposes that is located at his/her residence, please include information concerning these systems. [You will want detailed information about each computer (and manufacturer and model); name and version of all software, including operating system, private and custom developed applications, commercial applications and shareware, communications capability, 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.]
3. Provide the following information for each computer network in operation in the organization [You may want to limit this interrogatory to a particular department or subgroup]:
 - a) Name and version number of the network operation system in use;

- b) Quantity and configuration of all network servers and workstations;
 - c) Identity of the person(s) responsible for the ongoing operation, maintenance, expansion and upkeep of the network; and
 - d) Name and version of all application and other software residing on the network, including, but not limited to, electronic mail applications.
4. Provide the following for each mini- and mainframe computer system used in the organization:
- a) Name and version number of the operating system in use;
 - b) Identity of the person(s) responsible for the ongoing operation, maintenance, expansion and upkeep of the mini- and/or mainframe system; and
 - c) Name and description of function of all application and other software residing on the network, including, but not limited to, electronic mail applications.
5. Describe in detail all possible ways in which electronic data are shared between organizations, the method of transmission, type(s) of data transferred and the names of all individual possessing the capability for such transfer, including lists and names of authorized regular outside users of the [producing party's] electronic mail system.
6. Please provide the following information concerning data backups performed on all computer systems in the organization:
- a) Descriptions of any and all procedures and/or devices used to backup the software and/or data, including, but not limited to, name(s) of backup software used, tape rotation schedule, type of tape backup drives including name and version number;
 - b) Are multiple generations of backups maintained? If so, please describe how many and whether the backups are full or incremental;
 - c) Are backup storage media kept off-site? If so, where are such media kept? Describe the process for archiving and retrieving off-site media?
 - d) Are backup storage media kept on-site? If so, where are such media kept? Describe the process for archiving and retrieving on-site media;
 - e) Identify who conducts the backup, including name, title, office location, and telephone number;

- f) Describe, in detail, what information is backed up; and
- g) Please provide a detailed list of all backup sets, regardless of the magnetic media on which they reside, showing current location, custodian, date of backup and a description of backup content.

In some litigation, voice mail messages may be important. These may be more difficult to gain access to due to technical limitations in the voice mail service.

- 7. State whether users may store voice mail messages. If so, please provide the following information:
 - a) State whether users have the option of storing voice mail messages;
 - b) If users can store messages, state how long messages remain on the system? State how many messages may be stored by each user; and
 - c) State whether voice mail messages are automatically purged. If so, describe in detail the destruction schedule.

System Configuration:

- 1. Describe the types (including names and models) of computer system(s) used by your company in the course of business.
- 2. Describe/identify the name, type and version of software used on your computer system(s).
- 3. Identify the person(s) responsible for the ongoing operation, maintenance, expansion, backup and upkeep of the computer system.
- 4. Do employees have home computers used for business purposes? If yes, insert answers to questions 1-2 for computers used at home for business purposes.
- 5. Are passwords or encrypted files used on any of the computer systems?
 - a. If yes, describe how files are protected
 - b. Who could provide access codes if required?
 - c. Have you modified your use of computers to comply with recent discovery requests?
 - d. Have you deleted any files or other electronic documents since the filing of this lawsuit?

Backup and Retention:

1. List all computer systems in the organization that are backed up.
 - a. Describe the backup program(s) used (including information about legacy systems).
 - b. Give details of your backup procedures/protocols:
2. Have you modified or suspended your backup procedures/protocols to comply with recent discovery requests? If the answer is yes, please provide a detailed description of what has been done.
3. Are files ever deleted from the computer system(s) as part of backup/retention procedures?
4. Are archival backups ever created? If yes, what files have been archived? What are the archival backups maintained?
5. Describe any disaster recovery plans in place now and for the time period relevant to this lawsuit.

Maintenance and Access:

1. Are utility programs used on computer(s) in the office?
 - a. If yes: Which programs?
 - b. Has the program been used to permanently “wipe” files?
 - c. If yes, when?
 - d. Has the program been used to de-fragment, optimize or compress drives?
 - e. If yes, when?
2. If persons outside of the company can access the company computers, how do those outside of the company access the computers?
3. How are office computers secured?
4. Has any computer hardware been upgraded in the past 12 months?
5. Has any computer software been upgraded or replaced on office computers in the past 12 months?

Chain of Custody/Authentication:

1. Are individual directories purged when an employee leaves the company?
2. Are passwords and access codes revoked when an employee leaves the company?
3. Are workstations reassigned to incoming employees?
 - a. If yes, are hard drives wiped or re-formatted for the new user?
 - b. Are hard drives backed up before the new user uses the workstation?
4. Describe how used or replaced equipment is disposed of or sold.
5. Describe how used disks or drives are treated before destruction or sale, including whether they are degaussed or shredded.
6. Have you used outside contractors to upgrade either hardware or software?
 - a. If yes, please identify the contractors.
7. Are changes or modifications made to software recorded?
 - a. If yes, please describe the medium for recording, e.g., electronic.
 - b. Are hard copy logs kept?

Computer hardware:

1. List all computer equipment provided by [party name] or used by employees of [party name] to perform work for [party name], including but not limited to hardware/or peripherals attached to a computer such as computer cases [desktop, tower, portable/batteries, all-in-one], monitors, modems [internal, external], printers, keyboards, scanners, mice [cord and cordless], pointing devices [joystick, touch pad, trackball], speakers, include description of equipment, serial number, all users for the period _____ to _____ and dates used, and all locations where the equipment was located for the period _____ to _____.
2. Will [party name] permit, without an order therefore, inspection of the equipment described in the answer to the preceding interrogatory?
3. List all hardware components (e.g., motherboard, modem, NIC, etc.) installed internally or externally to the PC(s) used by _____ during the period _____ to _____.

4. List discarded or replaced hardware and software for the PC(s) (including entire PCs) used by _____ during the period _____ to _____. If the hardware or software is no longer in your control, state the name and contact information of the last known custodian.

Computer Software:

1. List any and all software installed or used on the PC(s) used by _____ during the period _____ to _____. Include all titles and version numbers. Include authors and contact information for authors of custom or customized software. Include Operating System(s) software.

Operating Systems:

1. List all operating systems (including but not limited to UNIX, Windows, DOS, Linux, and PDA operating systems) installed on all computers used by [party name], the specific equipment the Operating System was installed on, and the period during which it was installed on the specific equipment.

Telephone or Communication Systems:

1. Do you have any graphic representation of the components of the telephone and voice messaging system of [party name], and the relationship of those components to each other, including but not limited to flow charts, videos, photos, or diagrams?
2. If so, where are the documents located?
3. List all telephone equipment provided by [party name] or used by employees of [party name] to perform work for [party name], including but not limited to desktop telephones, cellular phones, pagers, PDA and laptop modems, calling cards, telephony software, and contact management software. Include description of equipment and software, serial number, all users of the period of _____ to _____, and dates used, and all locations where the equipment was located for the period of _____ to _____ inclusive.

Other Sources of Electronic Evidence:

1. List all log files (files with suffixes but not limited to . . . found on computers in [party name]'s network, and the equipment and logical path where the log files may be found.
2. Do any employees of [party name] subscribe to or participate in Internet newsgroups or chat groups in the course of their employment?

3. If yes, list all users and the services that they subscribe to or participate in.
4. Do any employees of [party name] use portable devices in the course of their employment that are not connected to [party name]'s network and which are not backed up in archives?
5. If so, list all users and the devices they use.
6. Do any employees of [party name] use portable devices in the course of their employment that are not connected to [party name]'s network and which are not backed up in archives?
7. If so, list all users and the devices they use.
8. Does [party name] provide Internet access for any of its employees or has [party name] does so at any time during the period from _____ to _____ inclusive/
9. If so, list the employees who had Internet access, the Internet service provide (ISP) used, and describe the method(s) used to connect to the Internet.
10. Describe any restrictions on, controls over, or monitoring of employee use of Internet resources.
11. Provide a list of any and all Internet-related data on the PCs used by [specific employees or classes of employees], including but not limited to save web pages, lists of web sites, URL addresses, Web browser software and settings, bookmarks, favorites, history lists, caches, cookies.

Data Security Measures:

1. List any and all user identification numbers and passwords necessary to access computers or programs addressed in interrogatories. Your response to this Interrogatory must be updated with responses to future sets of Interrogatories and updated responses to any set of Interrogatories.
2. Explain [party name]'s policies and procedures for protecting data.
3. Explain [party name]'s policy for application specific security settings.

Network Questions:

1. List any and all documents and things related to networks or groups of connected computers that allow people to share information and equipment, including but not limited to local area networks (LAN), wide area networks (WAN), metropolitan area networks (MAN), storage area networks (SAN), peer-to-peer networks, client-server networks, integrated services digital networks, virtual private networks (VPN).

2. List any and all documents related to networks, including but not limited to information exchange components (e.g., Ethernet, token-ring, ATM), network file servers, traffic, hubs, network interface cards, cables, firewalls, user names, passwords, Intranet.
3. Do you have any graphic representation of the components of your computer network, and the relationship of those components to each other, including but not limited to flow charts, videos, photos, or drawings.
4. If so, where are the documents located. Include logical paths for electronic documents.
5. List any and all information related to e-mail, including but not limited to, current, backed up and archived programs, accounts, unified messaging, server-based e-mail, web-based e-mail, dial-up e-mail, user names and addresses, domain names and addresses, e-mail messages, attachments, manual and automated mailing lists, mailing list addresses.

[Defendant/Plaintiff] during the time period relevant to the actions taken that constitute the basis for this lawsuit.

BACKGROUND

On _____, counsel for [Plaintiff/Defendant] sent a letter to [Defendant/Plaintiff] informing that [Plaintiff/Defendant] electronic data or compilations would be an important and irreplaceable source for discovery and/or evidence and that [Plaintiff/Defendant] intended to submit discovery requests to obtain documents and other information in electronic form and to access computer(s), computer network(s) and computer systems. (Attachment B) This letter reminded [Defendant/Plaintiff] that his/her obligation to preserve electronic data is the same as for other forms of evidence. Counsel for [Plaintiff/Defendant] requested that [Defendant/Plaintiff] safeguard against the destruction of evidence until final resolution of the litigation and listed eight (8) categories of electronic data that should be preserved.

After receipt of this letter and after commencement of this lawsuit, [Defendant/Plaintiff] has embarked on a course of conduct designed to hinder and delay and even destroy evidence that is relevant to this lawsuit. [For example, [Defendant's/Plaintiff's] records management program was not suspended and electronic documents have been deleted, or in the normal course of [Defendant's/Plaintiff's] ongoing disaster recovery program systems administrators have reused critical backup tapes and thereby overwritten discoverable information, or files have been deleted from the hard drives of critical desktop or laptop computers].

As part of the discovery in this lawsuit, [Plaintiff/Defendant] served a set of Requests for Production of Computer Equipment, electronic documents, software, and other items upon [Defendant/Plaintiff]. Each of the requests is narrow and directed to the issues relevant to this lawsuit, and none is overbroad or burdensome. [Defendant/Plaintiff] has refused to produce responsive material on the grounds that the requests are vague, ambiguous, overly broad and burdensome, and because they seek confidential and proprietary documents, as well as documents protected by attorney-client and work-product privileges. Since the filing of this lawsuit, [Defendant/Plaintiff] has knowingly permitted or contributed to the destruction of responsive evidence.

Counsel for [Plaintiff/Defendant] sent a letter to opposing counsel proposing a procedure to access [Defendant's/Plaintiff's] computers and servers. The procedure incorporated the parties' agreed Confidentiality Order for protection of attorney-client and work product privileges and protection of trade secrets and proprietary information. The procedure proposed by counsel provided:

1. Defendants and counsel will meet with plaintiffs' counsel with computer forensic expert and review each file on computer. This review will be conducted in a manner that does not disrupt plaintiffs' business.
2. If a file may lead to discovery of admissible evidence and is not protected from production by a privilege, it will be copied and produced.
3. A privilege log will be maintained of all documents withheld on basis of privilege.
4. If the parties conclude file may not lead to discovery of admissible evidence, it will not be produced.
5. Plaintiffs will use and pay for their own expert for this process. If defendants want a neutral expert, costs for the neutral expert will be shared equally.

Counsel for [Defendant/Plaintiff] rejected this proposal.

ARGUMENT

[Plaintiff/Defendant] put [Defendant/Plaintiff] on notice at the outset of this lawsuit that discovery would include electronic versions of documents. A party's duty to preserve relevant documents arises when a party has notice of the relevance. *Applied Telematics, Inc. v. Sprint Communications Co.*, 1996 U.S. Dist. LEXIS 14053 (E.D.Pa. September 17, 1996); *Turner v. Hudson Transit Lines, Inc.*, 142 F.R.D. 68 (S.D.N.Y. 1991); *see Civil Discovery Standards*, ABA Section of Litigation, at part IV, page 17 (August 1999).

[Plaintiff/Defendant] has a duty to suspend its ongoing records management or the reuse of backup tapes once the duty to preserve documents arises. *Lewy v. Remington Arms Co.*, 836 F.2d 1104 (8th Cir. 1988); *Applied Telematics, Inc. v. Sprint Communications Co.*, 1996 U.S. Dist. LEXIS 14053 (E.D.Pa. September 17, 1996);

[Plaintiff/Defendant] has no means to obtain the full content of documents prepared with the use of computer equipment other than by inspection of the equipment itself.

Under Federal Rule of Civil Procedure 26(b)(2)(i)-(iii), the interests of [Plaintiff/Defendant] outweigh those of [Defendant/Plaintiff]. *See Fennell v. First Step Designs, Ltd.*, 83 F.3d 526 (1st Cir. 1996). [Defendant/Plaintiff] will suffer no undue burden or prejudice from being required to comply with [Plaintiff's/Defendant's] document production request. On the other hand, absent compliance by [Defendant/Plaintiff] with its discovery obligations, [Plaintiff/Defendant] will be unable to effectively pursue its claims against [Defendant/Plaintiff] because, due to the inexcusable conduct of [Defendant/Plaintiff] relevant, material and non-privileged information will have been withheld from [Plaintiff/Defendant].

Federal Rule of Civil Procedure 34(a) provides, in pertinent part, that “[a]ny party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on the requestor’s behalf, to inspect and copy, any designated documents (including . . . data compilations).” *Bills v. Kennecott Corp.*, 108 F.R.D. 459 (D.Utah 1985).

The obligation to produce electronic versions of documents and records is not new. Since 1970, Federal Rule of Civil Procedure 34 has authorized a party to request production of designated documents in electronic form and the electronic source itself. *Advisory Committee Notes for the 1970 Amendments to Rule 34; Illinois Tool Works, Inc. v. Metro Mark Products, Ltd.*, 43 F.Supp.2d 951 (N.D.Ill. 1999).

The electronic version of a document contains valuable information that the hard copy does not provide. In *Armstrong v. Executive Office of the President*, 1F.3d 1274 (D.C.Cir. 1993), the court said that printing a hard copy of an e-mail message was not the same as preserving the electronic version because the hard copy does not contain directories, distribution lists, acknowledgment of receipts, or transmittal information. [A print out of a document or its appearance on a computer monitor may not indicate any change or what existed before the change. *Does Discovery of Electronic Information Require Amendments to the Federal Rules of Civil Procedures?* Commercial & Federal

Litigation Section, Committee on Federal Procedure, New York State Bar Association Report (February 22, 2001)].

Numerous recent court decisions have ruled that Rule 34 permits party to request production of a document in its electronic form and not merely rely on the hard copy of a document. In *Playboy Enterprises, Inc. v. Welles*, 60 F.Supp.2d 1050 (S.D.Cal. 1999), plaintiff requested access to defendant's hard drive to attempt to recover deleted files that may have been stored on the hard drive. The court determined that plaintiff's need for access outweighed the potential interruption to defendant's business and approved plaintiff's request. In *TY, Inc. v. Le Claire*, 2000 WL 1015934 (N.D.Ill. June 1, 2000), the court granted plaintiff's motion and authorized plaintiff, at its own expense, to inspect the hard drives of computers defendants used during the relevant time period. In *Simon Property Group v. mySimon, Inc.*, 194 F.R.D. 639 (S.D. Ind. 2000), the court granted plaintiff's motion to compel defendants to produce their computers so that plaintiffs could attempt to recover deleted computer files.

RELIEF REQUESTED

For these reasons stated, [Plaintiff/Defendant] respectfully requests that this Court enter an Order directing [Defendant/Plaintiff] to permit inspection and copying of certain computer equipment, computer storage devices, software and documents used by [Defendant/Plaintiff] during the time period relevant to the actions taken that constitute the basis for this lawsuit and directing [Defendant/Plaintiff] produce the designated computer equipment, software and documents within five (5) business days of this Order.