

**EIGHTEENTH ANNUAL
SOUTHERN SURETY AND FIDELITY CLAIMS
CONFERENCE**

**New Orleans, Louisiana
APRIL 12TH & 13TH, 2007**

**COMPUTERS WILL MAKE LIFE SIMPLIER, EASIER AND LESS
EXPENSIVE - RIGHT? . . . WELCOME TO E-DISCOVERY!**

PRESENTED BY:

**JOHN V. BURCH, ESQ.
GREGORY R. VEAL, ESQ.
BOVIS, KYLE & BURCH, L.L.C.
53 Perimeter Center East
Third Floor
Atlanta, Georgia 30346-2298
770-391-9100**

I. INTRODUCTION

With the expansion of the internet and wide-spread computer usage in our daily lives, a new problem is created concerning legal discovery of electronically stored information.¹ Electronically stored information affects every area of litigation, not just cases involving large corporations or white-collar crime. Electronic discovery issues will affect every counsel and every company.

The amendments to the Federal Rules of Civil Procedure concerning electronic discovery became effective on December 1, 2006. The proposed rule changes were unanimously and without objection approved by the Judicial Conference on September 20, 2005. The United States Supreme Court unanimously approved these rules without comment or dissent on April 12, 2006, and Congress abstained from intervening to implement the new rules. These amendments were designed to address the lack of standards and set guidelines in federal courts regarding electronic discovery. The foremost importance of the new rules is that it makes parties give early attention to electronic discovery issues², and brings discussions and disputes before the court in regards to electronically stored information. The Advisory Committee noted four main reasons for the enactment of the new amendments:

1. the volume of electronic data is exponentially greater than paper documents;
2. electronic data is dynamic and can be created, altered or destroyed;
3. unlike paper documents, electronic data is difficult, although not impossible, to delete; and
4. electronic data may need to be retrieved, restored or translated before it can even be reviewed for relevance or privilege.³

Electronic discovery, or e-discovery, refers to the discovery of electronic documents and data. Some examples of the sources of electronic data include: emails, instant messaging (IMs), and text messages. Electronic documents include GIF, JPEG, JFIF, PDF, DOC, ZIP files, backup files, temporary files, and DBF (database files).

Even before the new rules became effective, courts had referenced them in their decisions. For instance, in Phoenix Four v. Strategic Resources Corporation, 2006 WL 1409413 at *6 (S.D.N.Y. May 23, 2006), the court cited to the proposed amendment Rule 26 in requiring parties to disclose a “description by category and location of . . . electronically stored information.” The court in Phoenix Four held that parties must identify the sources of potentially relevant information, but need not produce unreasonably inaccessible data: “Proposed Rule 26(b)(2) reinforces the concept that a party must identify even those sources that are ‘not reasonably accessible,’ but exempts the party from having to provide discovery from such sources unless its adversary moves to compel discovery.”

¹ We are grateful for Kathy So, a law student at Georgia State University College of Law and law clerk at Bovis, Kyle & Burch, in connection with this paper.

² See Appendix B, Rule 26(f). The amended rules are attached as appendices.

³ Jonathan M. Hoff and Douglas I. Koff, *What Next in E-Discovery? New Amendments Offer Step Toward Uniformity But Questions Remain*, NYLJ, Volume 237 (February 20, 2007).

Even though no uniform approach to electronic discovery had been developed by the federal courts, several courts had already made decisions regarding electronic discovery before the new rules were implemented. For instance, in United States v. Philip Morris, 327 F. Supp. 2d. 21 (D.D.C. 2004), the district court in D.C. held that there was spoliation of electronically stored evidence. Specifically, the court in Philip Morris found that an order requiring the preservation of “all documents and other records containing information which could be potentially relevant to the subject matter of this litigation” included emails that were being deleted during the course of business. As a result of this non-compliance, the court required defendants to pay a monetary sanction of \$2.75 million, precluded testimony during trial of any individuals who had failed to comply with the document retention order, and were also ordered to reimburse the United States for costs associated with Rule 30(b)(6) depositions on email destruction issue. Many federal courts had treated electronic discovery in the same manner as paper discovery.⁴

Benefits of electronic discovery include speed, accuracy, cost savings in terms of less review hours, and narrowed data for future litigation. However, production of electronic information is costly and technological factors involved in electronic discovery can make the discovery process confusing. Moreover, there may be more exposure and inadvertent production.

II. EMERGENCE OF ELECTRONICALLY STORED INFORMATION (ESI)

One study reports that almost 800 megabytes of recorded information is produced per person each year, 92 percent of which is magnetically stored form on computers or computer storage media.⁵ In comparison to paper recorded information, it would take 30 feet of books to store the equivalent of 800 megabytes of information on paper.⁶ It is estimated that less than 3 percent of electronic information is ever converted into paper format.⁷

A. ESI: Privilege Concerns

Electronically stored information, or ESI, is retained in greater volume than hard-copy paper documents. Also, as noted earlier, electronically stored information is dynamic; it is easily changed and most often changed on a frequent basis. Moreover, when separated from the system that created it, electronically stored information may be incomprehensible.

Due to the fact that electronically stored information is exponentially greater in volume than hard-copy documents, costs and exposures are tremendous factors. Privilege determinations are more difficult; review for privileged information is more expensive and time-consuming, and there is an increase in likelihood that inadvertent production will occur. General costs associated with electronically stored information include the costs of producing

⁴ *Id.*

⁵ Peter Lyman and Hal R. Varian, *How Much Information 2003?* At <http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/> (last visited February 12, 2007). According to this report, the total production of all new information was 5 exabytes in 2002. Five exabytes of information is equivalent in size to half of all information in the Library of Congress. Paper information constituted 0.01 percent of the total production of information in 2002.

⁶ *Id.*

⁷ David Narkiewicz, *Two Books to Help you Avoid your Worst Nightmare*, Pennsylvania Lawyer, 29-FEB Pa. Law. 58 (Jan./Feb. 2007).

the information, and costs by the receiver to decipher through the information where there is an overwhelming amount of ESI used as a trial tactic.

B. Metadata

A printed hardcopy of electronically stored information loses certain aspects of the information. For instance, a printed copy of a Microsoft Word document will not include information about when the document was created, who created the document, when it was modified, or any other information regarding its metadata. As such, metadata creates a new complication with electronic information in regards to discovery. Metadata, or “data about data,” includes creation dates, modification dates, individuals who either accessed or worked on the data, and file location. Metadata is basically a fingerprint on the document and is generally not visible when the document is printed or when the document is converted to an image file.⁸ Usually, metadata is only available if accessed in its native format. For example, when a Word document is formatted into a PDF file, the metadata in the Word document will not be visible when viewing the document with a PDF viewer. Also, when viewing a Word document that has been printed out, there is no metadata information attached to the document. Software may also be used to remove metadata from electronic documents.⁹

Although, metadata is not explicitly addressed in the amendments, at least in one case, it was held to be discoverable. In Williams v. Sprint / United Management Company, 230 F.R.D. 640 (D. Kan. 2005), the court held that if a party is ordered to produce electronic documents as maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact, unless that party timely objects to the production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order.

C. “Deleting”

Moreover, simply hitting “delete” on the keyboard does not erase the electronically stored information forever. With paper documents, shredding the document will “delete” the information without a chance of recovering the exact document. However, unless the electronically stored information is overridden, it will remain and leave a trace in the electronic storage. When you “delete” an electronically stored information such as a computer file, the file becomes invisible to the operating system and the space occupied by the file is freed up for use, allowing the operating system to overwrite that space with new information. However, unless the operating system requires use of this space, overwriting does not immediately occur and the “deleted” data remains in your computer for a considerable time. Only upon overwriting the data does recovery of data become practically impossible.

The new rules purportedly address differences and the problems created by ESI by addressing the lack of standards and setting guidelines in electronic discovery. The new rules

⁸ Example of an image file is a PDF file. At times, a native format, or in which manner the electronically stored information was originally created, will not be accessible to outsiders or opposing parties; therefore, an image file that is easily viewed by others, such as a PDF file, will be created as an exact image of the original file. However, as mentioned, when an original file in its native format is converted to an image file, metadata will most likely be lost.

⁹ The process of removing metadata is commonly called “scrubbing” the electronic document.

make attorneys give early attention to electronic discovery issues. However, not all problems and issues regarding electronically stored information is addressed under the new rules.

III. THE NEW RULES

A. Brief Summary of the New Rules

The new rules: (1) prompt early discussion of issues relating to ESI¹⁰; (2) discuss production of ESI that is “not reasonably accessible”¹¹; (3) provide a procedure for when a party asserts an inadvertent production of privileged or protected information¹²; (4) direct production of ESI in native format unless otherwise agreed by the parties¹³; (5) address interrogatories and requests for production of ESI¹⁴; and (6) create a limited safe harbor for lost or destroyed electronic data.¹⁵

B. Early Attention to Electronic Discovery; Meet and Confer

Rule 16 now explicitly informs the court to the possible need to address the handling of discovery of electronically stored information early in the litigation.¹⁶ Rule 16(b)(5) specifies that “provisions for disclosure or discovery of electronically stored information” may be included in the scheduling order. This rule providing for a conference before the actual court trial gives discretion to enter an order adopting any agreements the parties reach for asserting claims of privilege or protection as trial-preparation material after inadvertent production in discovery.

Rule 26(a) amended the phrase “data compilation” to “electronically stored information,” so that now, the rule explicitly refers to ESI.¹⁷ Rule 26(f) discusses party conference and planning for discovery.¹⁸ Rule 26(f)(3) specifically discusses electronically stored information and the forms of production. Furthermore, Form 35, which is an official form as provided by F.R.C.P. 84, is amended to add parties’ proposals regarding disclosure or discovery of electronically stored information.¹⁹

Rule 26(f) mandates that 21 days before a scheduling conference or 21 days before a Rule 16(b) scheduling conference, the parties confer regarding discovery issues. The new rule adds that “any issues relating to disclosure or discovery of electronically stored information, including the form and forms in which it should be produced” may be developed to be included in the proposed discovery plan.²⁰ If electronically stored information is sought, the following information should be discussed: a discussion of each side’s information technology (IT) systems, including definitions; development of a discovery plan that contemplates each side’s system capabilities; preservation of electronic information; time frames for production;

¹⁰ See Appendices A, B, and G, Rules 26(f), 16(b), and Form 35.

¹¹ See Appendix B, Rule 26(b)(2)(B).

¹² See Appendix B, Rule 26(b)(5).

¹³ See Appendix D, Rule 34(b).

¹⁴ See Appendix C, Rule 33(d).

¹⁵ See Appendix E, Rule 37(f).

¹⁶ See Appendix A.

¹⁷ See Appendix B.

¹⁸ *Id.*

¹⁹ See Appendix G.

²⁰ Rule 26(f)(3).

accessibility or inaccessibility of data under new Rule 26(b)(2)(B); and form or forms of production.

C. Discovery into ESI that is Not Reasonably Accessible

Rule 26(b)(2)(B) provides that a party need not produce ESI that is not reasonably accessible because of undue burden or cost. However, even if there is a showing of undue burden or cost, the court may still order discovery if the requesting party shows good cause.

In 2003, before the new rules were implemented, a New York district court took on the issue of inaccessible electronic discovery and cost shifting. In Zubulake v. UBS Warburg LLC, 217 F.R.D. 309 (S.D.N.Y. 2003), the plaintiff moved for an order compelling the defendant to produce emails that allegedly included evidence to support her claim of gender discrimination and illegal retaliation. The defendant argued that restoring the emails would be unduly burdensome in terms of costs. The Zubulake court cited the United States Supreme Court case Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340 (1978): “the presumption is that the responding party must bear the expense of complying with discovery requests . . .” Moreover, the court modified an earlier ruling in the same court in Rowe Entertainment, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421 (S.D.N.Y. 2002), and set out seven standards in the order of importance to determine the appropriateness of cost-shifting:

1. The extent to which the request is specifically tailored to discover relevant information;
2. The availability of such information from other sources;
3. The total cost of production, compared to the amount in controversy;
4. The total cost of production, compared to the resources available to each party;
5. The relative ability of each party to control costs and its incentive to do so;
6. The importance of the issues at stake in the litigation; and
7. The relative benefits to the parties of obtaining the information.²¹

Although this guideline was set by one district court prior to the enactment of the new rules, since cost-shifting in electronic discovery has not been addressed in the new rules, the Zubulake decision may have a significant impact in this area of electronic discovery.

D. Procedure for Asserting Claims of Privilege and Work Product Protection after Production

Rule 26(b)(5) addresses the procedure for asserting claims of privilege and work product protection after production. If a party has produced information in discovery that it claims is privileged or protected as trial-prep material, it may notify the receiving party of claim,

²¹ See Zubulake, 217 F.R.D. at 322.

stating the basis for it. After receiving notification, the receiving party must return, sequester, or destroy the information, and may not use or disclose it to third parties. If there was disclosure before notification, the receiving party also must take reasonable steps to retrieve the information.

E. Interrogatories and Requests for Production of ESI

Rules 33, 34(a), and 34(b) address interrogatories and requests for production of electronically stored information. Rule 33 includes the term “electronically stored information” as related to business records.²² Rule 34(a) also adds the term “electronically stored information” as related to scope of production.²³ Rule 34(b)(ii) provides that if a request does not specify the form or forms for producing ESI, a responding party must produce the information in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable.²⁴

F. Sanctions for Certain Type of Loss of ESI

Rule 37(f) is a new subdivision of Rule 37 to add electronically stored information.²⁵ The new rule provides that absent exceptional circumstances, sanctions may not be imposed under the civil rules if electronically stored information sought in discovery had been lost as a result of the routine operation of an electronic information system, as long as that operation is in good faith. This rule responds to the distinctive and necessary feature of computer systems, i.e., the recycling, overwriting and alteration of electronically stored information that attends normal use.

IV. PRACTICAL CONSIDERATIONS UNDER THE NEW RULES

Some aspects of electronic discovery that are not addressed in the new rules but should still be considered include: tactical attention to meet and confer, means of preventing spoliation of evidence and preservation orders, and relying on “clawback” or “quick peek” agreements.

A. Meet and Confer

Prior to the Rule 26(f) party conference, not only attorneys but also the clients should become familiar with their information technology (IT) systems. Clients should consider the “where, who and when” questions: Where is the relevant data? Who are the key players? When did the duty attach for preserving the information, and when was the responsive data created? Also, clients should consider preservation issues.

During the Rule 26(f) meet and confer, parties should consider whether to agree to an inspection of each other’s systems by consultants to streamline the process. Parties should also consider the timeline of the discovery process and the possibility of agreeing to search terms or protocols to make the process more cost effective for everyone. Parties may also consider agreeing on a form or forms of production, such as agreeing to produce documents in

²² See Appendix C.

²³ See Appendix D.

²⁴ See Appendix D.

²⁵ See Appendix E.

native format, paper format, or image-file format. Moreover, there should be discussions on possible cost shifting of expenses incurred with electronic discovery.

B. Spoliation and Preservation Letter

There is a concern that businesses may be sanctioned because they were unaware of the technical steps necessary to keep relevant electronically stored information from being lost or deleted. As mentioned in the introduction section, in United States v. Philip Morris, 327 F. Supp. 2d. 21 (D.D.C. 2004), defendants were heavily sanctioned for their failure to preserve electronic documents.

Prior to commencing an action, or immediately thereafter, you may want to send a preservation letter warning the opposing party of possible spoliation of evidence, especially considering the dynamic nature of electronically stored information. A preservation letter is a warning letter to the opposing party providing notice not to destroy, alter, or conceal any paper or electronic files and other data generated by or stored in your client's computers and media storage media (for example, hard disks, floppy disks, backup tapes, Zip disks, CDs, DVDs, etc.) or any other electronic data, such as voice mail. A preservation letter should also be sent to all non-parties in possession of potentially relevant data.

Included in the preservation letter should be some form of consequences. For example, the preservation letter could include the following sentence: "Failure to comply with this letter can result in severe sanctions being imposed by a court for spoliation of evidence or potential evidence." The letter should also include a description of how the recipient is to meet this burden to preserve. For instance, by including the following sentences: "Providing the requested data on the original media, or on exact copies of that media (image, evidentiary, or mirror copies)" and "Suspending certain document destruction policies and computer maintenance procedures, including de-fragmenting hard drives, deleting internet cookies, deleting browser history and favorites, and running any 'disk clean-up' procedures."

The preservation letter should also fully provide a detailed description of the files and file types that must be preserved, for example:

- All emails, both sent and received, internal and external;
- All word processed files;
- All data created with the use of personal or portable data assistants;
- All internet and web-browser-generated history files;
- Caches and "cookie" files generated at the workstation of each employee; and
- Logs of network use.

A statement that the definition includes, but is not limited to the listed items, is appropriate.

Due to the ever-changing nature of electronic data, the timing of a preservation request may be critical. Consider sending the preservation letter before filing the complaint, which will provide the necessary notice to the opposing party and supply a possible basis for future sanctions.

C. “Clawback” or “Quick Peek” Agreements

Due to the greater volume of ESI than paper production, there is a greater chance of inadvertent production of privileged information. Moreover, since there is such a high volume of information stored electronically, costs associated with reviewing the documents would be substantially more than with paper documents. The Committee Note following Rule 26(f) explain the types of agreements that parties may enter into to avoid inadvertent waiver of privilege and suggest that they obtain court endorsement of any such agreement.

A “clawback” agreement refers to production of documents without intent to waive privilege of those documents. If a party inadvertently produces a privileged document, the production will not constitute a waiver, provided that the producing party identifies the documents mistakenly produced. Under a “quick peek” agreement, parties agree that the responding party will provide certain requested materials without having waived any privilege rights. However, these agreements may fail considering that they do not account for third parties and waiver of privilege is a substantive area of law that may vary depending on the jurisdiction.

V. CONCLUSION

Technology will continue to advance, and a paperless society may be emerging. The newly implemented federal rules addressing electronic discovery attempts to address the advances in technology; however, there are many issues not yet covered by the rules. In addition to the concerns previously mentioned, you may want to consider the following recommendations to assist your counsel in dealing with electronic discovery.

A. Recommended Tactics

The following are some recommended tactics to assist you with how to handle the new amendments²⁶:

- Update and enforce your records management policy;
- Adopt litigation early warnings strategies;
- Correct implementation of the litigation hold;
- Review computer use policies with electronic discovery in mind;
- Educate, Educate, Educate
- Adopt collection plans;
- Stay up to date.

²⁶ Arthur Smith, *E-Discovery Survival Guide for Corporate Counsel*, Mondaq Bus. Briefing (February 19, 2007).

i. Updating & Enforcing Records Management Policy

Foremost, establish “good faith” data loss. The “safe harbor” rule of Rule 37 will more likely apply when there is a corporate policy on retention and deletion of electronically stored information. A records management policy will allow employees to know what documents that they are required to keep and for how long. More importantly, by having a records management policy, if a document is destroyed, you may show justification for the destruction of the document if challenged in court. Also, there should be backup policy along with a document retention policy. Moreover, do not assume that your IT department will be able to shoulder the burden alone. It may be a costly mistake to be unprepared to electronic discovery.

ii. Adopting Early Litigation Strategies

Although it may be difficult to assess when litigation is “reasonably foreseeable,” there should be placed some type of system for upholding the preservation duty when triggered. Ask the “where, who and when” questions and create a chart to inform those individuals directly affected by the foreseeable or pending litigation.

Companies should be able to identify their sources of electronic evidence, locate the sources and be able to produce it.

iii. Implementing the Litigation Hold

In order to properly implement a litigation hold, you must provide detailed and adequate instructions to employees about the subject matter and document types involved in the hold. You must also follow up with the key employees and make sure that the documents involved in the subject matter of the litigation is being held; and, conduct periodic compliance checks to make sure the hold is being adhered to.

Not only is it important to establish a good faith basis for deletion of data, you must also ensure that there is procedure for quickly and reliably implementing a litigation hold.

iv. Reviewing Computer Use Policies

Make sure you know how to identify and retrieve data. Also, consider who has access to the data, and which users actually accessed the data. Review, and if needed, revise your computer use policies.

v. Educate, Educate, Educate

Not only must you know these rules, but educate the people in your IT department as well. Also, educate all individuals in your department about the corporate document retention and deletion policies.

vi. Adopting Collection Plans

Before litigation is even in sight, familiarize yourself with the IT infrastructure and systems of your company. Identify those individuals that may assist in retrieving data if necessary. If you do not know your system well, make sure you can immediately contact

someone who can quickly and reliably implement a collection plan for your electronically stored information.

vii. Staying up to Date

The new rules were just implemented and new court decisions regarding the rules are being published daily. Staying up to date is the key to making sure that your company and departments are conforming to the new obligations.

APPENDIX A

Rule 16. Pretrial Conferences; Scheduling; Management

(b) Scheduling and Planning. Except in categories of actions exempted by district court rule as inappropriate, the district judge, or a magistrate judge when authorized by district court rule, shall, after receiving the report from the parties under Rule 26(f) or after consulting with the attorneys for the parties and any unrepresented parties by a scheduling conference, telephone, mail, or other suitable means, enter a scheduling order that limits the time

- (1) to join other parties and to amend the pleadings;
- (2) to file motions; and
- (3) to complete discovery.

The scheduling order also may include

- (4) modifications of the times for disclosures under Rules 26(a) and 26(e)(1) and of the extent of discovery to be permitted;
- (5) provisions for disclosure or discovery of electronically stored information;
- (6) any agreements the parties reach for asserting claims of privilege or of protection as trial preparation material after production;
- (7) the date or dates for conferences before trial, a final pretrial conference, and trial; and
- (8) any other matters appropriate in the circumstances of the case.

The order shall issue as soon as practicable but in any event within 90 days after the appearance of a defendant and within 120 days after the complaint has been served on a defendant. A schedule shall not be modified except upon a showing of good cause and by leave of the district judge or, when authorized by local rule, by a magistrate judge.

APPENDIX B

Rule 26. General Provisions Governing Discovery; Duty of Disclosure

(a) Required Disclosures; Methods to Discover Additional Matter.

(1) **Initial Disclosures.** Except in categories of proceedings specified in Rule 26(a)(1)(E), or to the extent otherwise stipulated or directed by order, a party must, without awaiting a discovery request, provide to other parties:

- (A) the name and, if known, the address and telephone number of each individual likely to have discoverable information that the disclosing party may use to support its claims or defenses, unless solely for impeachment, identifying the subjects of the information;
- (B) a copy of, or a description by category and location of, all documents, electronically stored information, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses, unless solely for impeachment;

(b) **Discovery Scope and Limits.** Unless otherwise limited by order of the court in accordance with these rules, the scope of discovery is as follows:

(2) Limitations.

- (A) By order, the court may alter the limits in these rules on the number of depositions and interrogatories or the length of depositions under Rule 30. By order or local rule, the court may also limit the number of requests under Rule 36.
- (B) A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.
- (C) The frequency or extent of use of the discovery methods otherwise permitted under these rules and by any local rule shall be limited by the court if it determines that: (i) the discovery sought is

unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought; or (iii) the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues. The court may act upon its own initiative after reasonable notice or pursuant to a motion under Rule 26(c).

(5) Claims of Privilege or Protection of Trial-Preparation Materials.

- (A) Information Withheld.** When a party withholds information otherwise discoverable under these rules by claiming that it is privileged or subject to protection as trial preparation material, the party shall make the claim expressly and shall describe the nature of the documents, communications, or things not produced or disclosed in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the applicability of the privilege or protection.
- (B) Information Produced.** If information is produced in discovery that is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has and may not use or disclose the information until the claim is resolved. A receiving party may promptly present the information to the court under seal for a determination of the claim. If the receiving party disclosed the information before being notified, it must take reasonable steps to retrieve it. The producing party must preserve the information until the claim is resolved.

(f) Conference of Parties; Planning for Discovery.

Except in categories of proceedings exempted from initial disclosure under Rule 26(a)(1)(E) or when otherwise ordered, the parties must, as soon as practicable and in any event at least 21 days before a scheduling conference is held or a scheduling order is due under Rule 16(b), confer to consider the nature and basis of their claims and defenses and the possibilities for a prompt settlement or resolution of the case, to make or arrange for the disclosures required by Rule 26(a)(1), to discuss any issues relating to preserving discoverable information, and to develop a proposed discovery plan that indicates the parties' views and proposals concerning:

- (1) what changes should be made in the timing, form, or requirement for disclosures under Rule 26(a), including a statement as to when disclosures under Rule 26(a)(1) were made or will be made;
- (2) the subjects on which discovery may be needed, when discovery should be completed, and whether discovery should be conducted in phases or be limited to or focused upon particular issues;
- (3) any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced;
- (4) any issues relating to claims of privilege or of protection as trial-preparation material, including – if the parties agree on a procedure to assert such claims after production – whether to ask the court to include their agreement in an order;
- (5) what changes should be made in the limitations on discovery imposed under these rules or by local rule, and what other limitations should be imposed; and
- (6) any other orders that should be entered by the court under Rule 26(c) or under Rule 16(b) and (c).

APPENDIX C

Rule 33. Interrogatories to Parties

(d) Option to Produce Business Records. Where the answer to an interrogatory may be derived or ascertained from the business records, including electronically stored information, of the party upon whom the interrogatory has been served or from an examination, audit or inspection of such business records, including a compilation, abstract or summary thereof, and the burden of deriving or ascertaining the answer is substantially the same for the party serving the interrogatory as for the party served, it is a sufficient answer to such interrogatory to specify the records from which the answer may be derived or ascertained and to afford to the party serving the interrogatory reasonable opportunity to examine, audit or inspect such records and to make copies, compilations, abstracts, or summaries. A specification shall be in sufficient detail to permit the interrogating party to locate and to identify, as readily as can the party served, the records from which the answer may be ascertained.

APPENDIX D

Rule 34. Production of Documents, Electronically Stored Information, and Things and Entry Upon Land for Inspection and Other Purposes

(a) Scope. Any 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, copy, test, or sample any designated documents or electronically stored information – including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained — translated, if necessary, by the respondent into reasonably usable form, or to inspect, copy, test, or sample any designated tangible things which constitute or contain matters within the scope of Rule 26(b) and which are in the possession, custody or control of the party upon whom the request is served; or (2) to permit entry upon designated land or other property in the possession or control of the party upon whom the request is served for the purpose of inspection and measuring, surveying, photographing, testing, or sampling the property or any designated object or operation thereon, within the scope of Rule 26(b).

(b) Procedure. The request shall set forth, either by individual item or by category, the items to be inspected, and describe each with reasonable particularity. The request shall specify a reasonable time, place, and manner of making the inspection and performing the related acts. The request may specify the form or forms in which electronically stored information is to be produced. Without leave of court or written stipulation, a request may not be served before the time specified in Rule 26(d).

The party upon whom the request is served shall serve a written response within 30 days after the service of the request. A shorter or longer time may be directed by the court or, in the absence of such an order, agreed to in writing by the parties, subject to Rule 29. The response shall state, with respect to each item or category, that inspection and related activities will be permitted as requested, unless the request is objected to, including an objection to the requested form or forms for producing electronically stored information, stating the reasons for the objection. If objection is made to part of an item or category, the part shall be specified and inspection permitted of the remaining parts. If objection is made to the requested form or forms for producing electronically stored information — or if no form was specified in the request — the responding party must state the form or forms it intends to use. The party submitting the request may move for an order under Rule 37(a) with respect to any objection to or other failure to respond to the request or any part thereof, or any failure to permit inspection as requested.

Unless the parties otherwise agree, or the court otherwise orders:

- (i)** a party who produces documents for inspection shall produce them as they are kept in the usual course of business or shall organize and label them to correspond with the categories in the request;
- (ii)** if a request does not specify the form or forms for producing electronically stored information, a responding party must produce the information in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable; and

- (iii) a party need not produce the same electronically stored information in more than one form.

APPENDIX E

Rule 37. Failure to Make Disclosures or Cooperate in Discovery; Sanctions

(f) Electronically Stored Information. Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.

APPENDIX F

Rule 45. Subpoena

(a) Form; Issuance.

- (1) Every subpoena shall
 - (A) state the name of the court from which it is issued; and
 - (B) state the title of the action, the name of the court in which it is pending, and its civil action number; and
 - (C) command each person to whom it is directed to attend and give testimony or to produce and permit inspection, copying, testing, or sampling of designated books, documents, electronically stored information, or tangible things in the possession, custody or control of that person, or to permit inspection of premises, at a time and place therein specified; and
 - (D) set forth the text of subdivisions (c) and (d) of this rule.

A command to produce evidence or to permit inspection, copying, testing, or sampling may be joined with a command to appear at trial or hearing or at deposition, or may be issued separately. A subpoena may specify the form or forms in which electronically stored information is to be produced.

- (2) A subpoena must issue as follows:

- (C) for production, inspection, copying, testing, or sampling, if separate from a subpoena commanding a person's attendance, from the court for the district where the production or inspection is to be made.

- (3) The clerk shall issue a subpoena, signed but otherwise in blank, to a party requesting it, who shall complete it before service. An attorney as officer of the court may also issue and sign a subpoena on behalf of

- (A) a court in which the attorney is authorized to practice; or
- (B) a court for a district in which a deposition or production is compelled by the subpoena, if the deposition or production pertains to an action pending in a court in which the attorney is authorized to practice.

(b) Service.

(1) A subpoena may be served by any person who is not a party and is not less than 18 years of age. Service of a subpoena upon a person named therein shall be made by delivering a copy thereof to such person and, if the person's attendance is commanded, by tendering to that person the fees for one day's attendance and the mileage allowed by law. When the subpoena is issued on behalf of the United States or an officer or agency thereof, fees and mileage need not be tendered. Prior notice of any commanded production of documents and things or inspection of premises before trial shall be served on each party in the manner prescribed by Rule 5(b).

(2) Subject to the provisions of clause (ii) of subparagraph (c)(3)(A) of this rule, a subpoena may be served at any place within the district of the court by which it is issued, or at any place without the district that is within 100 miles of the place of the deposition, hearing, trial, production, inspection, copying, testing, or sampling specified in the subpoena or at any place within the state where a state statute or rule of court permits service of a subpoena issued by a state court of general jurisdiction sitting in the place of the deposition, hearing, trial, production, inspection, copying, testing, or sampling specified in the subpoena. When a statute of the United States provides therefor, the court upon proper application and cause shown may authorize the service of a subpoena at any other place. A subpoena directed to a witness in a foreign country who is a national or resident of the United States shall issue under the circumstances and in the manner and be served as provided in Title 28, U.S.C. § 1783.

(3) Proof of service when necessary shall be made by filing with the clerk of the court by which the subpoena is issued a statement of the date and manner of service and of the names of the persons served, certified by the person who made the service.

(c) Protection of Persons Subject to Subpoenas.

(1) A party or an attorney responsible for the issuance and service of a subpoena shall take reasonable steps to avoid imposing undue burden or expense on a person subject to that subpoena. The court on behalf of which the subpoena was issued shall enforce this duty and impose upon the party or attorney in breach of this duty an appropriate sanction, which may include, but is not limited to, lost earnings and a reasonable attorney's fee.

(2) (A) A person commanded to produce and permit inspection, copying, testing, or sampling of designated electronically stored information, books, papers, documents or tangible things, or inspection of premises need not appear in person at the place of production or inspection unless commanded to appear for deposition, hearing or trial.

(B) Subject to paragraph (d)(2) of this rule, a person commanded to produce and permit inspection, copying, testing, or sampling may, within 14 days after service of the subpoena or before the time specified for compliance if such time is less than 14 days after service, serve upon the party or attorney designated in the subpoena written objection to producing any or all of the designated materials or inspection of the premises – or to producing electronically stored information in the form or forms requested. If objection is made, the party serving the subpoena shall not be entitled to inspect, copy, test, or sample the materials or inspect the premises except pursuant to an order of the court by which the subpoena was issued. If objection has been made, the party serving the subpoena may, upon notice to the

person commanded to produce, move at any time for an order to compel the production, inspection, copying, testing, or sampling. Such an order to compel shall protect any person who is not a party or an officer of a party from significant expense resulting from the inspection, copying, testing, or sampling commanded.

(3) (A) On timely motion, the court by which a subpoena was issued shall quash or modify the subpoena if it

- (i)** fails to allow reasonable time for compliance;
- (ii)** requires a person who is not a party or an officer of a party to travel to a place more than 100 miles from the place where that person resides, is employed or regularly transacts business in person, except that, subject to the provisions of clause (c)(3)(B)(iii) of this rule, such a person may in order to attend trial be commanded to travel from any such place within the state in which the trial is held;
- (ii)** requires disclosure of privileged or other protected matter and no exception or waiver applies; or
- (iv)** subjects a person to undue burden.

(B) If a subpoena

- (i)** requires disclosure of a trade secret or other confidential research, development, or commercial information, or
- (ii)** requires disclosure of an unretained expert's opinion or information not describing specific events or occurrences in dispute and resulting from the expert's study made not at the request of any party, or
- (iii)** requires a person who is not a party or an officer of a party to incur substantial expense to travel more than 100 miles to attend trial, the court may, to protect a person subject to or affected by the subpoena, quash or modify the subpoena or, if the party in whose behalf the subpoena is issued shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship and assures that the person to whom the subpoena is addressed will be reasonably compensated, the court may order appearance or production only upon specified conditions.

(d) Duties in Responding to Subpoena.

(1) (A) A person responding to a subpoena to produce documents shall produce them as they are kept in the usual course of business or shall organize and label them to correspond with the categories in the demand.

(B) If a subpoena does not specify the form or forms for producing electronically stored information, a person responding to a subpoena must produce the information in a form or forms in which the person ordinarily maintains it or in a form or forms that are reasonably usable.

(C) A person responding to a subpoena need not produce the same electronically stored information in more than one form.

(D) A person responding to a subpoena need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or to quash, the person from whom discovery is sought must show that the information sought is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

(2) (A) When information subject to a subpoena is withheld on a claim that it is privileged or subject to protection as trial-preparation materials, the claim shall be made expressly and shall be supported by a description of the nature of the documents, communications, or things not produced that is sufficient to enable the demanding party to contest the claim.

(B) If information is produced in response to a subpoena that is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has and may not use or disclose the information until the claim is resolved. A receiving party may promptly present the information to the court under seal for a determination of the claim. If the receiving party disclosed the information before being notified, it must take reasonable steps to retrieve it. The person who produced the information must preserve the information until the claim is resolved.

(e) Contempt. Failure of any person without adequate excuse to obey a subpoena served upon that person may be deemed a contempt of the court from which the subpoena issued. An adequate cause for failure to obey exists when a subpoena purports to require a nonparty to attend or produce at a place not within the limits provided by clause (ii) of subparagraph (c)(3)(A).

APPENDIX G

Form 35. Report of Parties' Planning Meeting

3. Discovery Plan. The parties jointly propose to the court the following discovery plan: [Use separate paragraphs or subparagraphs as necessary if parties disagree.]

Discovery will be needed on the following subjects: (brief description of subjects on which discovery will be needed)

Disclosure or discovery of electronically stored information should be handled as follows: (brief description of parties' proposals)

The parties have agreed to an order regarding claims of privilege or of protection as trial-preparation material asserted after production, as follows: (brief description of provisions of proposed order).

All discovery commenced in time to be completed by _____ (date) _____.
[Discovery on _____ (issue for early discovery) _____ to be completed by _____ (date) _____.]

APPENDIX H

FORM FOR PRESERVATION OF EVIDENCE LETTER

RE: DATA PRESERVATION - [IDENTIFY ISSUES]

Dear [Name]:

Please be advised that we have reason to believe that electronic information in your company's control or possession may be relevant to the issues and legal disputes arising out of [describe].

You and your company may have in your custody, possession or control documents, information and electronically or digitally stored data relevant to this dispute. In addition, you and your employees may have knowledge of facts related to this dispute.

You are under a legal duty to preserve, retain and protect all reasonably relevant and possibly relevant evidence, including the electronic evidence, once litigation appears imminent or has commenced. The failure to preserve or retain the electronic data outlined in this notice constitutes spoliation of evidence and will subject you to legal claims for damages or evidence and monetary sanctions.

For purposes of this notice, "electronic data" or "electronic evidence" shall include but is not limited to, all text files (including word processing documents), presentation files (such as PowerPoints), spreadsheets, e-mail files and information concerning e-mail files including logs, header and deleted file information, internet history files, preferences, graphical files in any format, data bases, calendar, scheduling information, task lists, telephone logs, contact managers, computer system activity logs, and all file fragments and backup files containing electronic data.

Specifically, you are instructed not to destroy, devise, erase, encrypt, alter or allow to be corrupted or otherwise make unavailable any electronic evidence relevant to the above-referenced dispute. You are further instructed to take reasonable efforts to preserve such data. To meet this burden, you are instructed, by way of example and not limitation, to:

- preserve all data storage backup files (i.e., do not overwrite any previously existing backups);
- preserve and retain all electronic data generated or received by employees who may have personal knowledge of the facts in this dispute;
- refrain from operating or removing fixed or internal drives, any work stations or laptops that are reasonably thought to have any data related to this dispute, including the workstations and laptops of _____;
- preserve and retain all data from servers and networking equipment logging network access activity and system authentication;

- preserve and retain all electronic data in any format, media or location related to this dispute, including data on floppy disks, zip disks, CD-ROM's, CD-WR's, tape, PDA's, cell phones, memory cards, sticks, or digital copiers;
- prevent employees from deleting or overwriting any electronic data; and
- take such measures including, but not limited to, restricting physical electronic access to all electronically stored data directly or indirectly related to the claim.

Thank you for your cooperation.

Sincerely,