

# **E-Discovery Rules**

Michael T. Coutu & Russell J. Fenton

**Sliwa and Lane**

**Michael T. Coutu, Esq.**

Law Offices of Sliwa & Lane

840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203

Tel.: (716) 853-2050 • Facsimile: (716) 853-2057

E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

## **Introduction**

Before anything meaningful can be said, a few preliminary points must be made. First, electronic discovery (e-discovery), is a growing parallel along side of technology, and this presentation will most likely be “out-of-date” by the time it’s finished.

Second, e-discovery is very expensive, and while it offers a few advantages in terms of evidence that previously could only be dreamt of, it is also having a dramatic effect on the average cost of litigation. Experts estimate that as much as 95% of a lawyer’s daily communications take place in a form other than paper. Traditionally, trial lawyers have been able to anticipate what type of records or other evidence must exist in paper format. From there they could then build their cases and have a reasonable idea of what, if anything, the other side could possibly discover.

E-discovery changes everything. Suddenly confidentiality battles usually only fought over written documents, and the occasional conversation, is now being fought with rigor over individual e-mails, and whether or not you may list an entire e-mail strand (conversation) as one entry on a privilege log, or whether you have to list each and every e-mail.

Then there is the data. If it has ever been typed or clicked on a computer, and the hard drive has not been smashed to pieces, it can, and will be recovered by computer experts. Judges are beginning more and more pre-trial conferences with questions

**Michael T. Coutu, Esq.**

Law Offices of Sliwa & Lane

840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203

Tel.: (716) 853-2050 • Facsimile: (716) 853-2057

E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

regarding whether or not the parties can agree on a type of data (Metadata, PDF, Tiff, etc.), that is compatible with their client's information storing system.

There are three forms in which data can generally be produced:

- 1) In its **native** form, that is when the document is produced in the file format it was created, with all metadata in tact;
- 2) In an **Image** form, such as a portable digital file (pdf) or tagged image file format (Tiff); and finally,
- 3) Good old **Paper**.

Effective December 1, 2006, the Federal Rules of Civil Procedure were significantly amended to acknowledge that litigation now takes place in an entirely different context than thirty years ago. The amendments that went into effect attempt to accommodate changes in information technology that have occurred and will continue in the future.

Interestingly, the fact that courts have been applying the proposed amendments before they became effective illustrates the need for further guidance regarding how to handle electronic discovery (see, Lee H. Rosenthal, The Yale Law Journal Pocket Part, pp 167-199 at 167). Due to the need to be flexible enough to apply in all federal cases and deal with changes in technology, the rules present procedures and policies to help resolve issues that arise, yet little in the way of concrete, case or specific rules or directives.

**Michael T. Coutu, Esq.**  
Law Offices of Sliwa & Lane  
840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
E-Mail: [mcoutu@sliwa-lane.com](mailto:mcoutu@sliwa-lane.com)

## DEFINITIONS

Before we get started, perhaps a few technological definitions and illustrations of their potential impact are in order.

### **i. Metadata**

Simply stated, metadata is data about data, and includes all the contextual, processing, and use information needed to identify and certify the scope, authenticity, and integrity of active or archival electronic information or records. Metadata is data that is not necessarily seen by viewing the face of the document, but remains hidden within the electronic version. To see an example of metadata, drag an e-mail attachment to your desktop. Right click on the file and rename it with the extension “.txt” instead of the usual “.wpd” or “.doc”. When you open the document in the notepad program, it shows you the raw code for the document, which includes the imbedded data.

### **ii. Why do I care about Metadata?**

In Plasse v. Tyco Electronics Corp., 448 F.Supp.2d 302 (D.Mass. 2006), a former employee of Tyco was terminated. In his later claim, a dispute developed about whether or not Plasse had misrepresented his credentials on the resume he submitted to Tyco. Eventually, Tyco’s computer expert was permitted to take a forensic image of Plasse’s computer. The recovered resume showed that the plaintiff had attempted to alter the data: “File metadata revealed that the retrieved file was accessed and modified on June

**Michael T. Coutu, Esq.**

Law Offices of Sliwa & Lane

840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203

Tel.: (716) 853-2050 • Facsimile: (716) 853-2057

E-Mail: [mcoutu@sliwa-lane.com](mailto:mcoutu@sliwa-lane.com)

28, 2005, then deleted at some unknown date between June 28, 2005, and the date on which the computer was produced, July 26, 2005". Plasse 448 F.Supp.2d at 306.

As far as practicable, there should be a direct connection between the form of production requested and the substantive needs of the case. The type of proof, the elements of the claim, and the connection to the data requested will be critical in this analysis. The connection between form and substance is important for two primary reasons: 1) the lawyer's goal should always be to "facilitate the orderly, efficient, and cost-effective discovery," as the drafters intended, Fed.R.Civ.P. 34, 2006 Advisory Committee Notes; and 2) if the responding party objects, and the lawyer engages in motion practice the judge is likely to ask the requesting party why the requested form is critical to the case. The most persuasive answers will be specific and case-based.

In the e-discovery battle of the forms, specificity wins. This principle is demonstrated by the seminal case of Williams v. Sprint/United Management Co., 230 F.R.D. 640 (D.Kan. 2005). In Williams, Magistrate Judge Waxse ordered an employer defending an age discrimination claim in the context of a reduction in force ("RIF") to produce certain spreadsheets relating to the RIF. Id. at 642-644. When the RIF spreadsheets were produced, the requesting party complained that "prior to producing the electronic versions of the Excel spreadsheets, the responding party had utilized software to scrub the metadata." Id. at 644. Moreover, the responding party had locked certain cells and data on the Excel spreadsheets prior to producing them so that the requesting

**Michael T. Coutu, Esq.**

Law Offices of Sliwa & Lane

840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203

Tel.: (716) 853-2050 • Facsimile: (716) 853-2057

E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

party could not access those cells.” Id. In other words, the requesting party complained that the spreadsheets were not produced in its unaltered native form.

In ordering the native production, the judge specifically noted that the requesting party had provided substantive explanation for why the metadata would be relevant to the claims in the case:

“In light of the Plaintiff’s allegations that Defendant reworked pools of employees in order to improve its distribution to pass its adverse impact analysis, the Court finds that some of the metadata is relevant and likely to lead to the discovery of admissible evidence... The Court does find that metadata associated with any changes to the spreadsheets, the dates of any changes, the identification of the individuals making any changes, and other metadata from which Plaintiffs could determine the final versus draft version of the spreadsheets appear relevant.”

Id. at 653.

The Plaintiffs were able to provide the Court with the specific reasons that the unaltered native production was important to the facts of that case. As a result, the Plaintiffs were successful in their “form” request.

### **iii. Image Production**

There are generally two predominate forms of image production files, they are PDF’s and TIFF files. A .tiff file (“TIFF”) is an “image” or “picture” of the document and an index with OCR (Optical Character Recognition), and possibly a tool for reviewing metadata. OCR is required with the TIFF format in order to make the document searchable. This means that a text version of the document is produced along with the TIFF format. Also, because TIFF files are typically single pages, an index is

**Michael T. Coutu, Esq.**  
Law Offices of Sliwa & Lane  
840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

critical to understand where document breaks occur. Conversion into a TIFF format can streamline the review process; however, it can also result in the loss of potentially important metadata if protocols for extraction are not agreed upon before conversion and production. It is advised that parties should agree to production in TIFF, with negotiable metadata fields (e.g., author, creation date, recipient, etc.). Alternatively, the parties could also agree to produce in TIFF, and the producing party simply maintains the metadata for later review should that become necessary.

Documents produced in .pdf (portable document format, PDF) are produced in a format which is an Adobe technology for formatting documents, and can be viewed and printed using a free reader available at adobe's website. The key to a usable PDF production is making it "searchable". The PDF must either be saved as searchable, or be OCR'd (optical character recognition, OCR) in order to be searchable. Again, metadata must be discussed because it can be lost by conversion and production in this format.

#### **I. An Overview of the E-Discovery Rules and Amendments:**

Perhaps the most important and far-reaching change to the rules is the introduction of the term: "Electronically Stored Information" which is generally referred to as "ESI." ESI is to be broadly construed to include anything in electronic form from e-mails to databases to spreadsheets to draft documents to internet activity. The new rules make a distinction between "documents" and ESI because documentary discovery and ESI discovery require different discovery management. Thus, through this distinction, and the implicit understanding that documents and ESI are different, the

**Michael T. Coutu, Esq.**  
Law Offices of Sliwa & Lane  
840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

drafters of the amendments were able to amend the rules to specifically address the issues peculiar to electronic discovery.

The electronic discovery amendments address five areas:

1. The Rule 26 conference --- Parties' obligation to meet and confer about electronic discovery early in the litigation process, including the need to preserve electronically stored information;
2. Discovery of information that is NOT reasonably accessible and allocating costs of that discovery;
3. Privilege review;
4. Preserving and Form of Producing E-Discovery; and
5. Sanctions.

## **II. Why do we Care?**

Both litigants and lawyers must concern themselves with E-discovery for at least three primary reasons. First, electronically stored information or ESI is pervasive and makes up the vast majority of all discoverable material. Thus, it would be truly short sighted to put blinders on and fail to explore this fertile, yet expansive area of potentially case breaking proof. Second, because ESI is everywhere and is, in the absence of privilege or immunity, clearly discoverable, and because it is not stored or kept in a manner that we are all used to, such as archiving of documents, attorneys and parties to a lawsuit or a potential lawsuit must know what ESI is, where to obtain it, how to keep it, when to preserve it and how to produce it in proper form without waiving any privilege.

**Michael T. Coutu, Esq.**

Law Offices of Sliwa & Lane

840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203

Tel.: (716) 853-2050 • Facsimile: (716) 853-2057

E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

Third, the cost of non-compliance, even if unintentional, significantly outweighs the costs of learning about electronically stored information and efficiently managing e-discovery. In other words, there are severe sanctions for failing to follow the rules, including rules regarding the obligation to preserve ESI prior to suit. Sanctions range from the simple striking of a pleading to monetary sanctions of a *billion* dollars or more.

For example, all twelve federal circuits have sanctioned parties' negligent or otherwise improper e-discovery conduct. Of note, the D.C. Circuit fined Philip Morris \$2.75 million for failing to abide by a preservation order and destroying emails in a fraud and racketeering case.

A \$1.45 *billion* judgment (\$604 million compensatory, \$850 million punitive), plus ongoing interest charges in excess of \$200 million, was recently entered against Morgan Stanley for E-discovery abuses. The judge in that case instructed the jury to assume that Morgan Stanley participated in a scheme to mislead and hide information because it repeatedly violated the judge's e-discovery orders by failing to produce emails.

In another recent case, a \$29.3 million judgment was entered in favor of a former employee in the context of a sex discrimination claim. In response to the defendant's failure to preserve and produce emails, the court instructed the jury to assume that any emails destroyed by the defendant after the plaintiff brought her claim would have been detrimental to the defendant's case. This jury charge likely had a great impact on the case, in light of the jury's verdict.

**Michael T. Coutu, Esq.**  
Law Offices of Sliwa & Lane  
840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

Therefore, it is imperative that the process of preserving electronically stored information begins as soon as litigation is reasonably anticipated.

### **III. The E-Discovery Amendments.**

On December 1, 2006, the Federal Rules of Civil Procedure (hereinafter the “FRCP”) were amended to address the disclosure of electronically stored information. The following rules were affected by the amendments: FRCP 16, 26, 33, 34 and 45.

#### **A. FRCP 26 --- Meeting & Conferring**

The amendments to FRCP 26 pertain to the necessary attention parties need to pay to e-discovery issues and how to better manage the disclosure of electronically stored information. The amended rules require parties to include electronically stored information in initial disclosures, the mandated early discovery planning conference of counsel, the report to the court and the pretrial scheduling conference with the Court.

#### **1. Initial Automatic Disclosure of Electronically Stored Information**

FRCP 26(a)(i) now includes electronically stored information in its list of information that must be initially disclosed by the parties. At the onset of litigation, each party must disclose a description, by category and location, of electronically stored information that the party may use to support its claims or defenses. Additionally, the name and contact information of each individual likely to have discovery information that the disclosing party may use to support its claim(s) or defense(s), and identifying the

**Michael T. Coutu, Esq.**  
Law Offices of Sliwa & Lane  
840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

subject(s) of the information, must be disclosed.

## **2. Electronic Discovery at the Early 30-Day Discovery Planning Conference**

At the early discovery planning or Rule 26(b) conference, the parties are to discuss disclosure of electronically stored information, including the form in which such information is to be produced. Issues such as the time period for which discovery will be sought and the topics for such discovery should be addressed. The parties are to agree on an e-discovery plan concerning “any issues relating to the disclosure of electronically stored information, including the form or forms in which it should be produced.” Counsel must “discuss any issues relating to preserving discoverable information and to develop a proposed discovery plan that indicates the parties’ views and proposals concerning: ... any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced.”

One judge focused on counsels’ obligation to plan appropriate discovery of electronically stored information at the Rule 26(b) conference when setting forth the “minimum” that should be discussed at the conference to include the following:

- the type of information technology system in use, and the persons most knowledgeable in their operation;
- preservation of electronically stored information that may be relevant to the litigation;
- the scope of the electronic records sought (i.e. e-mail, voice mail, archived data, back-up or disaster

**Michael T. Coutu, Esq.**

Law Offices of Sliwa & Lane

840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203

Tel.: (716) 853-2050 • Facsimile: (716) 853-2057

E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

recovery data, laptops, personal computers, PDA's, deleted data)[;]

- the format in which production will occur (will records be produced in “native” or searchable format, or image only; is metadata sought);
- whether the requesting party seeks to conduct any testing or sampling of the producing party's IT system;
- the burdens and expenses that the producing party will face based on the Rule 26(b)(2) factors and how they may be reduced (i.e. limiting the time period for which discovery is sought, limiting the amount of hours the producing party must spend searching, compiling and reviewing electronic records, using sampling to search, rather than searching all records, shifting to the requesting party some of the production costs);
- the amount of pre-production privilege review that is reasonable for the producing party to undertake, and the measures to preserve post-production assertion of privilege within a reasonable time; and,
- any protective orders or confidentiality orders that should be in place regarding who may have access to information that is produced.

(Hopson v. Mayor of Baltimore, 232 F.R.D. 228, at 245 [D. Md. 2005]) (referencing then proposed Rule 26(b)(5)(2) and the Civil Discovery Standards for the American Bar Association Section on Litigation).

Clearly, while not everything on the list will apply in every case, the amendments increase the demands on lawyer and litigant early in the litigation. That said, the lawyer must be prepared to discuss at the early discovery planning meeting(s): (1) the form of

**Michael T. Coutu, Esq.**

Law Offices of Sliwa & Lane

840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203

Tel.: (716) 853-2050 • Facsimile: (716) 853-2057

E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

production (so that choices can be made as to which of a variety of forms best suits the production of the particular information); (2) data preservation; and (3) privilege waiver. To do so effectively, counsel must know about: the client's information system, the sources and content of discoverable electronically stored information, how the information is created; how the information is stored; how it can be accessed and produced, and when it will, in the ordinary course become less accessible, lost, or modified.

### **3. Data Preservation**

Inasmuch as electronically stored information is dynamic, it is more complicated to decide what needs to be preserved and how to preserve it. For example, the ordinary operation of a computer, including just turning it on can alter or destroy associated electronically stored information. In other words, computer systems automatically create, alter, discard or overwrite data, without notice to the operator. Further, information may be deleted, yet continue to exist somewhere, but is difficult to locate or access. Thus, steps must be taken to preserve electronically stored information that would in the absence of affirmative effort be altered or destroyed automatically.

Specifically, the following should be addressed by counsel at the initial conference:

- the extent of the preservation obligation, including the types of material to be preserved, the subject matter, time frame, the authors, addressees and key words to be used in identifying responsive materials;

**Michael T. Coutu, Esq.**  
Law Offices of Sliwa & Lane  
840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

- the form and method of providing notice of the duty to preserve to the custodians of the information;
- identification of those responsible for carrying out preservation obligations on behalf of each party;
- plans for monitoring, certifying or auditing compliance with preservation obligations; whether preservation will require suspending or modifying any routine business processes or procedures, with special attention to document management programs and the recycling of computer data storage devices; methods to preserve any volatile but potentially discoverable material, such as voicemail, active data in databases or emails and instant messages; and
- the anticipated costs of preservation and ways to minimize or share the costs; and a method to review and modify the preservation duty as discovery proceeds, eliminating or adding particular categories of information.

#### **4. Litigation Holds**

To meet the preservation obligations, parties who reasonably anticipate litigation or who have been sued generally use “litigation holds” to prevent the loss of information that may later be demanded in discovery. A sample litigation hold letter is included at the end of these materials.

The amendments seek to help the parties balance the risk of an overly broad litigation hold (expensive and time consuming) against the cost of failing to preserve discoverable information (spoliation and sanctions), by requiring the parties to discuss the issues early and, where necessary, obtain judicial clarification before it is too late, and the information destroyed or lost.

**Michael T. Coutu, Esq.**

Law Offices of Sliwa & Lane

840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203

Tel.: (716) 853-2050 • Facsimile: (716) 853-2057

E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

## **B. POST PRODUCTION PRIVILEGE & PRIVILEGE WAIVER**

It is more difficult, time consuming and expensive to identify and segregate privileged, work product, trade secret, copyright, license materials and material prepared in anticipation of litigation that may well be contained within electronically stored information than with paper discovery.

Moreover, due to limits of technology and the technology-human interphase there is an increased risk of inadvertent disclosures even with costly pre-production privilege reviews. Because a failure to screen out even one privileged item may result in an argument that the privilege has been waived regarding all materials related to the same subject matter, parties may feel it necessary to engage in extraordinarily aggressive pre-production privilege reviews. However, Amended Rules 26(b) and 16 discuss approaches to assert claims of privilege or work-product protection post-disclosure. In fact, “Clawback agreements,” which pertain to the inadvertent disclosure of privileged information and the lack of waiver resulting from the same, should be discussed at the early discovery planning meeting. Moreover, if the parties agree on protocols to facilitate faster and cheaper discovery, the court can include the agreement in the case management order. If an agreement cannot be reached, the parties are directed to seek early judicial resolution of these issues.

Further, FRCP 26(b)(5)(B), as amended, permits a party who has inadvertently produced privileged information to get the information back or have the other party destroy it until the privilege claim is resolved. The amended rule recognizes that

**Michael T. Coutu, Esq.**  
Law Offices of Sliwa & Lane  
840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

protecting against the inadvertent disclosure of privileged information is more difficult with electronically stored information since the volume is so much greater and access to the plethora of forms of ESI is varied (See e.g., Hernandez v. Standard Oil Co., 2006 W.L. 1967364 [D.P.R. July 11, 2006]).

If privileged information is inadvertently produced, under the amended rules, the party asserting the privilege claim must notify the receiving party in writing and specifically identify the information along with the privilege it is claiming. This must be sufficiently detailed for the court and the receiving party to be able to understand the basis of the claim and whether waiver has occurred. When the party with the privileged information receives such notice, it must destroy, sequester or return the information and retrieve the information already provided to third parties. It may not use the information pending resolution of the privilege claim.

However, the judge still retains broad discretion to decide whether the privilege has been waived. Some courts, however, appear to be rather unsympathetic. Even as recently as July 2006, a mere three months before the amended rules became effective, a court observed that even where an errant mouse click results in the inadvertent disclosure of privileged information, the privilege is waived (Hernandez, 2006 W.L. 1967364 at 4). The court noted that even “if parties opt to use technological resources to store privilege information, they should be provided the necessary protection for precisely that information” (Hernandez, 2006 W.L. 1967364 at 4; see also, Bowles v. Nat’l Ass’n of Home Builders, 224 F.R.D. 246, 243 [D.D.C. 2004] [strict rule on waivers]). By

**Michael T. Coutu, Esq.**

Law Offices of Sliwa & Lane

840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203

Tel.: (716) 853-2050 • Facsimile: (716) 853-2057

E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

contrast, other courts are more lenient with regard to inadvertent waiver, and some have found some middle ground that requires the court to assess whether the conduct that led to the production was excusable (see e.g., Hapson, 252 F.R.D. 228 at 231-244 (balancing test and explanation of all other costs); Helman v. Murry's Steaks, Inc., 728 F.Supp.1099, 1104 [D. Del. 1990] [lenient rule]; United States v. Rigas, 281 F.Supp. 2d. 733, 737 [S.D. N.Y. 2003] [balancing test]).

Regardless, through the amendments to Rule 26(f) and 26(b)(5)(B), as amplified by the Committee Notes, which acknowledge the difficulty of conducting privilege reviews of vast amounts of electronically stored information, the courts have a basis to become more forgiving. Still courts cannot force parties to enter into clawback, quick peek or any other protocol, even if the same would expedite and reduce the expense of discovery. This obviously, and in the absence of an agreement, leaves counsel in the very difficult position of having to assume that any inadvertently disclosed privileged material, may well waive that privilege, and litigants must be kept informed of these risks before and during the discovery phase of any litigation.

There is also the issue of whether waiver extends to third parties. This problem arises, in part, out of the judicial reluctance to enforce non-waiver agreements upon third parties (see, Roth at p. 184). There is however, a proposal for a rule change that would provide that if the court enters an order incorporating the parties' non-waiver agreement as allowed for under Rule 26(f) and Rule 16, the order would bind third parties. The proposed rule also adopts the middle ground approach to privilege waiver (see Report of

**Michael T. Coutu, Esq.**  
Law Offices of Sliwa & Lane  
840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

the Advisory Committee on Evidence Rules 4 [amended June 30, 2006]).

### **C. Not Reasonably Accessible Information and Cost Allocation**

The drafters of the amended rules recognize the burden and expense of producing electronically stored information, some of which may well not be readily accessible. Rule 26(b)(2), as amended, applies a two-tiered structure to address this problem. At the first tier, the parties must disclose reasonably accessible, electronically stored information, without a court order. At the second tier, electronically stored information that is “not reasonably accessible” need not be reviewed or produced, unless the requesting party can show good cause for a court to order production. Instead, the responding party must disclose the existence of electronically stored information that is likely to contain relevant information located on sources that are not reasonably accessible.

#### **1. Identification**

Again, FRCP 26(b)(2), as amended, protects litigants from incurring undue expense by allowing parties at the early discovery planning stage to “identify, by category or type, the sources containing potentially responsive information that it is neither searching nor producing” because of the undue burden or expense it would incur in producing information from sources it identifies as not reasonably accessible. In other words, the responding party can identify the existence of the information available that may or may not include relevant discoverable material, but need not produce it unless the court directs the party to do so. When taking this position, the responding party must set

**Michael T. Coutu, Esq.**

Law Offices of Sliwa & Lane

840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203

Tel.: (716) 853-2050 • Facsimile: (716) 853-2057

E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

forth with specificity the burdens that it would incur if required to produce the information, including the likelihood of locating responsive information. Of course, should judicial intervention be required, the party responding to the discovery demands has the burden of demonstrating that the information sought is “not reasonably accessible.” In such cases, courts have started to use and/or require “not reasonably-accessible logs,” similar to a privilege log, to address the identification problem.

## **2. What is NOT Readily Accessible**

The Committee Notes to the amended rules identify the following as potential sources of electronically stored information that are not readily accessible:

- Un-indexed backup tapes intended for disaster recovery that are subject to electronic searching;
- legacy data from obsolete computer systems that is unreadable on the party’s current system; and
- deleted information maintained in fragmented form that would require specialists to restore.

## **3. Sampling Authorized to determine “Accessibility”**

Naturally, the party seeking the discovery does not know what lurks within the abyss of the “not readily accessible” and may need access to the information allegedly “not reasonably accessible” in order to properly reply to the producing party’s argument. The amended rules permit parties to request an opportunity to “sample” another party’s electronic information system. Sampling is defined by the American Bar Association as

**Michael T. Coutu, Esq.**  
Law Offices of Sliwa & Lane  
840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

“the process of testing a database for the existence or frequency of relevant information.” While sampling does not create direct access, it allows the party seeking discovery to determine what the alleged inaccessible sources contain and how difficult it would be for the responding party to retrieve the information. Sampling can be useful to determine discovery related issues, such as which data repositories are appropriate to search in certain litigation and to determine the effectiveness of other data extraction procedures.

#### **4. Not Reasonably Accessible Is Still Discoverable for “Good Cause”**

In determining whether to require the production of electronically stored information that the responding party has identified as not reasonably accessible, courts apply the following approach. First, the court must determine whether the information is indeed “not reasonably accessible.” If the information is not reasonably accessible, the party requesting the information must show “good cause” for the discovery. That is, the requesting party has to prove that the information sought is within the scope of discovery and is being requested in good faith.

#### **5. Reducing the Burden of Producing “Not Reasonably Accessible” ESI**

If the court determines that the information is sought in good faith and is within the scope of discovery, the court may still order the production of the information, even if is not reasonably accessible. However, the court may require the requesting party to incur all or part of the costs of the production pursuant to FRCP 26(b)(2)(C).

**Michael T. Coutu, Esq.**  
Law Offices of Sliwa & Lane  
840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

Of course, this was always within the court's power to shift costs of burdensome discovery. For example, in Zubulake v. UBS Warburg, (216 F.R.D. 280 [S.D.N.Y. 2003]) the court applied a seven (7) part analysis to determine which party should incur the costs of restoring allegedly inaccessible computer data and searching it for responsive information. Factors considered by the court include: (1) the specificity of the request; (2) the quantity of information available from more easily accessed sources; (3) the responding party's failure to produce information that likely existed on more easily accessed sources, but is no longer available from such sources; (4) the probability that responsive information, which cannot be obtained from other, more easily accessed sources, will be obtained; (5) the probability that the sought information will be useful; (6) the importance of the issues at stake in the litigation; and (7) the parties' respective resources.

After performing the analysis, the court determined that the responding party should bear 75% of the cost of restoring the information and searching it for responsive material. The cost of attorneys' fees for searching for privileged information within this material was incurred by the responding party. The court reiterated that cost-shifting is only appropriate when allegedly inaccessible information is being requested.

Further, there is an emerging question that has arisen where a party who properly preserved electronically stored information by saving the information on sources that are not readily accessible attempts to shift costs under Rule 26(b)(2)(B). For example, in Quinby v. Westle AG, the court held that an employer in an employment dispute case

**Michael T. Coutu, Esq.**  
Law Offices of Sliwa & Lane  
840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

would not be sanctioned, but could NOT shift the cost to the plaintiff to obtain and restore e-mails that the employer had, as a matter of pre-claim ordinary business practice, deleted and archived on a tape back-up system (Quinby v. Westle AG, 2006 W.L. 2597900 at 8-9 [S.D.N.Y Sep 5, 2006]). By contrast, in an earlier case titled Treppel v. Biovail Corp., the Southern District of New York found that storing information in a less accessible format was sanctionable because it did not meet a party's preservation obligation. Thus, potential litigants must draw a very fine line to meet preservation obligations, and apparently hope that the line is drawn in a location that allows them to both avoid sanctions, and possibly recover costs for restoring information that is not accessible.

The amendment to the Rules simply seem to codify the court's decision in Zubulake. Through the explicit discussion of cost shifting within the amendment, the Rules now make it clear that discovery of electronically stored information, even if it is NOT reasonably accessible, may be had regardless of the cost of production. That said, the requesting party should be prepared to pay the costs of production to offset the producing party's expense of production.

#### **D. FORM OF PRODUCTION -- FRCP 33 & 34**

Rule 33, the rule governing interrogatories to parties, was amended to include electronically stored information. The amendment perhaps states the obvious, and clarifies the transparent by providing that the electronic-discovery equivalent of answering an interrogatory by referring to business records is for the responding party to

**Michael T. Coutu, Esq.**  
Law Offices of Sliwa & Lane  
840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

provide access to electronically stored information, if the interrogatory party can find the answer as readily as the responding party.

Similarly, the amendments clarified and expanded Rule 34, which dealt with the production of documents and things, to include the production of electronically stored information. Before the amendment, “documents” and “tangible things” were discoverable under the rule requiring the production of documents and things. Where case law has interpreted “documents” to include “electronically stored information,” the amendment leaves no question.

In addition, the Rule tracks the meet and confer requirements for parties to discuss the form of production, and provides a procedure for court resolution of the form of production. The procedure for requesting disclosure now permits a party to request another party to specify the form(s) in which the electronically stored information is to be produced. FRCP 34(b). If the request does not specify the form(s) for the production of electronically stored information, the responding party must produce the information in the form(s) in which it is ordinarily maintained or in a form(s) that is “reasonably usable.” FRCP 34(b)(ii). The responding party can produce the information in multiple forms if no single form will suffice for all requested information. The responding party can, of course, object to the requesting party’s specification of form and suggest what form(s) it proposes to use.

Case law interpreting this section directs that the party who responds to discovery demands by producing electronic information as kept in the ordinary course of business

**Michael T. Coutu, Esq.**  
Law Offices of Sliwa & Lane  
840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

bears the burden of demonstrating that the information was indeed produced in that manner (DE Technologies, Inc. v. Dell, Inc., 238 F.R.D. 561 [W.D.Va. 2006]).

FRCP 34(b)(iii), as amended, directs that a party need not produce the same electronically stored information in more than one form. For example, email attachments can be produced separately from the emails to which they were attached (Williams v. Sprint/United Management Co., 2006 W.L. 3691604 [D.Kan. 2006]).

Further, not all electronic data has a counterpart in hard copy form. “Metadata” is a term used to describe “data about data” or information describing the history, tracking, or management of a document, or any other sort of “hidden” information about electronic files. Any information concerning the management or history of electronically stored information, is now unquestionably subject to disclosure. The problem of course for courts, lawyers and litigants is that now, attorneys and litigants must be incredibly detailed in attending to production issues, and that the court’s oversight and supervision of discovery is likewise going to be more detailed and invasive with e-discovery than it was with paper discovery.

#### **E. FRCP 37 – “Safe Harbor” from Spoliation Sanctions**

Rule 37(f) is a new rule that limits a court’s authority to sanction a party under the civil rules for failure to produce information in discovery, if, in the absence of exceptional circumstances, information is “lost as a result of the routine, good-faith operation of an electronic information system.” This “safe harbor” provision provides that the court cannot impose sanctions for a party’s failure to produce information that

**Michael T. Coutu, Esq.**

Law Offices of Sliwa & Lane

840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203

Tel.: (716) 853-2050 • Facsimile: (716) 853-2057

E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

was “lost as a result of the routine, good-faith operation of an electronic information system.” Per the Committee Note to the amended rule, the “routine operation” of computer systems refers to the alteration and overwriting of information, possibly without the operator’s express intent or awareness.

The rule does allow the court to impose sanctions in “exceptional circumstances” without regard to whether the loss of information was due to the good faith operation of an electronic information system. One of the factors considered in determining whether the party acted in good faith is whether it complied with the agreement entered into concerning e-discovery during the initial conference. Also, this rule does not apply to sanctions that can be imposed pursuant to rules of professional responsibility.

Rule 37, as amended, is an attempt to address the distinct feature of electronic information systems which through normal use modify, overwrite and delete information. After all, unlike documents, electronically stored information is certain to be lost in the absence of affirmative efforts to retain it. Thus, the risk of losing information that may be demanded in discovery is particularly problematic for electronically stored information. This has caused both small and large data producers who are often the subject of claims (insurers, utilities, etc.), to over-preserve due to uncertainty and the fear of spoliation sanctions. The over-preservation leads to over-production, which, in turn further drives up the cost in both time and dollars of electronic discovery, as well as the likelihood of unintentionally disclosing privileged material. Rule 37 is an attempt to provide certainty to data producers and limit the cost of over-preservation by reducing the

**Michael T. Coutu, Esq.**

Law Offices of Sliwa & Lane

840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203

Tel.: (716) 853-2050 • Facsimile: (716) 853-2057

E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

fear of spoliation sanctions, so long as the information is merely lost in good faith through the routine use of the electronic system. Finally, Rule 37 forces judges to analyze spoliation claims involving electronically stored information with the understanding that electronically stored information, unlike information on paper, which requires an affirmative act of destruction, is destroyed automatically.

#### **F. FRCP 45 – SUBPOENAS & ESI**

FRCP 45 adds electronically stored information to the type of information ascertainable by subpoena. This rule applies to entities that operate computer networks for litigants. Such entities are increasingly subpoenaed for information about a party's computer use.

Like FRCP 34, this rule permits the production of information in the form ordinarily maintained by the party or in a form that is “reasonably useable.” Absent good cause, the responding party need not produce the same information in more than one form. As in FRCP 26(b)(2)(C), the responding party need not provide information from sources that are not reasonably accessible, unless the court orders otherwise. The sampling provision of FRCP 34 is included in the amended FRCP 45 to permit sampling of information allegedly not reasonably accessible. The amended rule also includes a “claw back” provision for the retrieval of privileged information inadvertently produced.

#### **IV. SPOILATION – THE COST OF FAILING TO PRESERVE**

Spoliation is the failure of a party to properly preserve information subject to disclosure. It can result in serious adverse consequences. Penalties for spoliation can be

**Michael T. Coutu, Esq.**  
Law Offices of Sliwa & Lane  
840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

extreme and include monetary fines (*i.e.*, \$20,000 for intentionally deleting files [Advantacare Health Partners, LP v. Access IV (N.D.Ca. 2004)]), dismissal of claims and defenses, costs for supplementary discovery or adverse jury instructions. When imposing sanctions, courts generally consider the intent and behavior of the producing party and the degree of prejudice caused by the spoliation.

To avoid spoliation, a “litigation hold” should be imposed as soon as a party knows or should know that information that could lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery or is subject to a pending discovery request.

In other words, once litigation is reasonably anticipated, routine document destruction, electronically stored information wasting, must be suspended and a litigation hold imposed. Once the litigation hold is imposed, all potentially relevant information must be identified and made subject to the litigation hold. It is not enough to notify employees to save the information; active steps must be taken to ensure that relevant information is not being destroyed. Because the duty to supplement discovery responses is ongoing, litigation hold instructions should be reissued periodically to ensure that the litigation hold is continuous.

The fact that electronically stored information is not reasonably accessible does not relieve a party of its duty to preserve the information if potentially relevant.

Generally, the litigation hold is not applicable to inaccessible backup tapes that are used solely for disaster recovery. Such tapes can continue to be recycled according to

**Michael T. Coutu, Esq.**  
Law Offices of Sliwa & Lane  
840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

the schedule set forth in the company's policy. If, however, backup tapes are accessible, that is, used for information retrieval, they must be made subject to the litigation hold. Backup tapes containing the information of key players in the litigation (or anticipated litigation) should be preserved if this information is not available from other sources and if it is ascertainable where on the backup tapes the key players' information is located.

Once a litigation hold is imposed, the party and counsel must ensure that all sources of potentially relevant information are identified and preserved. To do that, counsel must be fully familiar with the client's document retention policies and the client's electronic information retention structure.

In Zubulake v. UBS Warburg, LLC (2004 W.L. 1620866 [S.D.N.Y. 2004]) ("Zubulake V"), the court reiterated counsel's duty to communicate to clients clearly and effectively the client's duty to preserve and produce all relevant electronically stored information on an ongoing basis. In addition, independent of the client's obligations, counsel has an obligation to take steps to safeguard backup tapes, request information from key employees and give litigation-hold instructions to the client's key employees. Failure to do so could result in a finding that there has been spoliation of evidence.

Once potentially relevant information is identified, there is a continuing duty to retain and produce the information if it is non-privileged and responsive to the requesting party's discovery demands. Counsel must meet with the key players involved in the litigation, explain the preservation obligation and periodically reiterate that the

**Michael T. Coutu, Esq.**  
Law Offices of Sliwa & Lane  
840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

preservation duty is continuous throughout the litigation. All employees should be instructed to produce electronic copies of their relevant active files. Counsel must also make sure that all backup media the party is required to retain is identified and safely stored. In appropriate cases, counsel should take possession of the backup tapes.

In Zubulake v. UBS Warburg, LLC, 220 F.R.D. 212 (S.D.N.Y. 2003) (“Zubulake IV”), the court addressed the preservation obligations of the parties. Once a party reasonably anticipates litigation, it must suspend its routine information retention/destruction policy and put in place a "litigation hold" to ensure the preservation of relevant information. As a general rule, the litigation hold does not apply to inaccessible backup tapes (*e.g.*, those typically maintained solely for the purpose of disaster recovery), which may continue to be recycled on the schedule set forth in the company's policy. On the other hand, if backup tapes are accessible (actively used for information retrieval), such tapes should be made subject to the litigation hold. If a company can identify where particular employees' documents are stored on backup tapes, then the tapes storing the documents of key players to litigation should be preserved if the information contained on those tapes is not otherwise available.

**Michael T. Coutu, Esq.**

Law Offices of Sliwa & Lane

840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203

Tel.: (716) 853-2050 • Facsimile: (716) 853-2057

E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

In Optowave Co., Ltd. v. Nikitin (2006 W.L. 3231422 [M.D.Fla. 2006]), the court imposed sanctions for the party's failure to retain responsive information. In determining whether to impose spoliation sanctions, the court reviewed the responding party's Microsoft Outlook file and found that some of the messages indicated that reply emails had been sent, but the reply emails were not produced. The court found that the missing emails were either intentionally deleted or were lost when the company's computer server was reformatted. This reformatting was performed by a computer consultant after the party had notice that a claim would be asserted against it.

The court imposed sanctions. In doing so, it noted the sophistication of the responding party with regard to advanced computer technology. It found that the party whose computer server was reformatted should have known that this process would create a loss of documents. It failed to preserve the data before the reformatting, even though on notice of the potential lawsuit. It also was given express notice of its duty to preserve evidence. Accordingly, the court found that the party acted in bad faith by allowing relevant evidence to be destroyed. It stated:

Sanctions may be imposed against a litigant who is on notice that documents and information are relevant to litigation, or potential litigation, or are reasonably calculated to lead to the discovery of admissible evidence, and destroys such documents and information. While a litigant is under no duty to keep or retain every document in its possession once a complaint is filed, it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery, and/or is the subject of a pending discovery request (citations omitted).

**Michael T. Coutu, Esq.**  
Law Offices of Sliwa & Lane  
840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

In Zubulake v. UBS Warburg (216 F.R.D. 280 [S.D.N.Y. 2003]), the court determined how to penalize the responding party for spoliation. The restoration of backup tapes was previously ordered by the court. Following this, the parties determined that certain backup tapes were missing and that certain emails were deleted after the litigation hold was imposed. The court pointed out that a party can only be punished for spoliation if it had a duty to preserve the evidence. The litigation hold applies to documents currently in existence and to documents created thereafter.

The court ruled that an adverse jury charge, which is a possible spoliation remedy, was not appropriate. It used a three (3) part test in making this determination. The party seeking the adverse jury charge must have control over the evidence when it was destroyed and must have had a duty to preserve it at that time. The documents must have been destroyed with a “culpable state of mind.” Finally, the destroyed materials must have been relevant to a party’s claim or defense. Destroying evidence in bad faith is sufficient to demonstrate the relevance of the evidence.

The court found that the party that destroyed the information was merely negligent because the issue of preservation of backup tapes was still a gray area at the time. The court found that the party’s alleged belief that backup tapes could be recycled was understandable. Also, there was insufficient proof that the deleted emails would support the requesting party’s claims. Thus, the adverse jury charge was found inappropriate. The court’s remedy was to allow the party requesting the information to re-depose certain witnesses on the issues of evidence destruction. The responding party had to bear the costs of these depositions.

**Michael T. Coutu, Esq.**

Law Offices of Sliwa & Lane

840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203

Tel.: (716) 853-2050 • Facsimile: (716) 853-2057

E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

In Zubulake v. UBS Warburg (2005 W.L. 627638 [S.D.N.Y. 2005]), the defendant moved for an order directing that the court's previous decisions in this case, which included the imposition of sanctions for spoliation, not be placed before the jury. The court granted the motion, finding the previous decisions irrelevant, but maintained that if the defendant opened the door by introducing evidence concerning whether their failure to produce was reasonable, the plaintiff could then introduce correspondence between counsel concerning the discovery dispute.

An extensive discussion of e-discovery is found in Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc. (2007 W.L. 684001 [D. Colo. 2007]). Here, the plaintiff moved for relief from the alleged discovery violations of the defendants. Numerous discovery disputes were at issue, including spoliation. The plaintiff sought various materials, including electronic communication documents and day-timer information. The defendant had an automatic email destruction program, pursuant to which emails older than ninety (90) days would be automatically destroyed.

The court recognized that interrupting automatic features of electronic information systems can be expensive and burdensome:

It is unrealistic to expect parties to stop such routine operation of their computer systems as soon as they anticipate litigation. It is also undesirable; the result would be even greater accumulation of duplicative and irrelevant data that must be reviewed, making discovery more expensive and time consuming.

The defendant argued that it instituted a litigation hold within days of the lawsuit and that its employees were directed not to destroy or delete documents related to the

**Michael T. Coutu, Esq.**  
Law Offices of Sliwa & Lane  
840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
E-Mail: [mcoutu@sliwa-lane.com](mailto:mcoutu@sliwa-lane.com)

litigation. It was the defendant's practice to expunge the hard drives of former employees once they left the company. The court found that this procedure with respect to employees "who played a significant or decision-making role in issues relevant to the litigation" violated the defendant's obligation to preserve evidence. No attempt was made by the defendant to contact its former employees with regard to the plaintiff's discovery demands.

The defendant conceded that it never reviewed the information on its backup tapes for discovery purposes. Plaintiff argued that the defendant failed to conduct "system wide keyword searches." The court recognized that it would be extremely burdensome to conduct a keyword search of the backup tapes. As to the electronic daily planners, the court required the defendant to certify that it conducted a search of all such reasonably accessible information for both current and former employees involved in the issues relevant to the litigation. Finally, the court directed the defendant to provide a declaration describing its efforts to review its website for responsive materials.

In Ameriwood Industries, Inc. v. Liberman (2006 W.L. 3825271 [E.D.Mo. 2006]), in response to a discovery dispute, the court directed the parties to retain an expert consultant. In this employment discrimination case, the computers were used to facilitate some of the alleged wrongdoings.

The court began its analysis of the amended FRCP 34(a) by pointing out that the requesting party does not have the right to search through all of the responding parties' records. It added that the sampling language in the amended rules was not intended to

**Michael T. Coutu, Esq.**  
Law Offices of Sliwa & Lane  
840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

give a right of direct access to the responding party's electronic information system. It acknowledged that such access may be justified occasionally, but noted that it is the court's responsibility to protect the parties from unnecessary intrusion. Also, the expert consultant was to review the computers and/or hard drives that were retained by the parties at their homes.

The request for all documents "describing or identifying" electronic databases that the employer maintained containing personnel related information was found to be overly broad. The court limited this request to databases containing personnel related information to avoid retrieval of documents that even fleetingly referenced personnel related information.

#### **V. E-DISCOVERY IN NEW YORK STATE COURTS**

The most important difference between e-discovery in New York State and federal court is that in New York State, the party seeking the information incurs the cost. As discussed above, in federal court, a cost-shifting analysis that considers the seven (7) factors enumerated in Zubulake may be imposed with regard to information production.

Additionally, the New York State Civil Practice Laws and Rules ("CPLR") do not address e-discovery. Accordingly, the following discussion of e-discovery in New York State is limited to case law.

New York courts tend to be somewhat more practical with regard to resolving e-discovery disputes. For example, in Etzion v. Etzion (7 Misc.3d. 940, 796 N.Y.S2d 844 [Sup. Ct., Nassau County 2005]), a matrimonial case in Nassau County, the court ruled

**Michael T. Coutu, Esq.**  
Law Offices of Sliwa & Lane  
840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

that the plaintiff was entitled to information stored on her husband's computer. To effectuate the disclosure process of this information, the court directed that a "clone" of the computer hard drive be created. The parties' experts and a court-appointed referee were to then examine the records, with the referee maintaining control of the records until the conclusion of the litigation.

In Lipco Electric Corp. v. ASG Consulting Corp. (4 Misc.3d. 1019(A), 798 N.Y.S.2d 345 [Sup. Ct., Nassau County 2004]), the court acknowledged the various issues that arise in connection with electronic discovery, including whether documents have been deleted, whether documents are still available on computer hard drives and/or backup tapes and whether software used to access the documents is licensed specifically for the user.

Per the court, the first step in addressing discovery is to determine whether the material sought is "material and necessary" to the prosecution or defense of the action. Once the court has ruled that certain information is discoverable, it must determine who should bear the cost of discovery. The court acknowledged that in federal court, the party from whom electronic discovery is sought bears the expense so long as it is unduly burdensome. In New York State, however, the party seeking the discovery generally bears the costs incurred in the production of the material in the absence of an agreement or court order.

The party responding to the discovery demands, ASG, used customized software for billing. It asserted that the information sought could not be retrieved without the

**Michael T. Coutu, Esq.**  
Law Offices of Sliwa & Lane  
840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

assistance of a computer consultant. Also, in order to produce some of the information, ASG argued that a separate program would have to be created to search for and extract the requested information. Then, once the information is found, counsel would have to review the same to determine whether it is subject to discovery. The court directed the parties to provide a detailed analysis of the procedures involved in retrieving the information and the costs that would be incurred.

Sampling was ordered by the court in Delta Financial Corp. v. Morrison (13 Misc.3d 604, 819 N.Y.S.2d 908 [Sup. Ct., Nassau County 2006]). Here, the defendant sought electronic information from the plaintiff. With regard to the backup tapes it sought, the defendant argued that such tapes are subject to disclosure, regardless of why they were created and that as long as the information is accessible, it must be produced. The plaintiff disagreed, arguing that backup tapes maintained only for purposes of disaster recovery, as opposed to storage of electronic information for purposes of routine retrieval, are not subject to discovery unless the requesting party can demonstrate “a need and relevance that outweigh the cost, burden, and disruption” of retrieving the data. The court directed the plaintiff to restore some of the backup tapes to provide a sample of the information stored therein. The requesting party was ordered to pay for the costs of same, including attorneys’ fees incurred in reviewing the records for privileged information.

Finally, it is important to note that in DeVita v. Macy’s East, Inc., 36 A.D.3d 751, 828 N.Y.S.2d 531 [2d Dept. 2007]), the court ruled that e-mail does not suffice for a

**Michael T. Coutu, Esq.**  
Law Offices of Sliwa & Lane  
840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

settlement stipulation because CPLR 2104 requires that all stipulations be written and subscribed to by those bound.

## **VI. A Practical Approach to Managing E-Discovery**

### **A. Identification and Location of Potentially Discoverable Material**

Information that may be requested during discovery includes organizational charts for the company's information technology department; written policies, procedures or guidelines developed for backup or emergency restoration of electronic information, including backup tape rotation schedules; written policies, procedures or guidelines used concerning electronic data retention, preservation or destruction, including schedules related to those procedures; employee use policies concerning company computers and other technology; policies and guidelines for naming and labeling files, disk and other information storage devices; policies regarding email storage; policies regarding the maintenance of electronic data generated by or concerning former employees; policies regarding home computer usage of employees; agreements for services by a computer technician regarding data that was stored, retrieved, downloaded, restored, removed, deleted or extracted; and documents relating to the chain of custody of computer drives examined or copied by a computer specialist with regard to data that was restored, retrieved, downloaded, removed, deleted or salvaged.

Once potentially responsive information is identified, it must be located on the storage devices and computer systems. Then, it must be retrieved from the computer

**Michael T. Coutu, Esq.**  
Law Offices of Sliwa & Lane  
840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

hardware or software housing the data and preserved. The information is then analyzed for responsiveness and sorted for privilege. Finally, the information is produced to the requesting party with a privilege log.

To prepare for the possibility of having to respond to discovery demands seeking electronically stored information, companies should create or modify their policy on storage and destruction of electronically stored information. Knowing where information is stored or whether it has been destroyed pursuant to document retention policies will avoid the high costs associated with e-discovery. To ensure compliance with said policy, periodic audits should occur. This will prevent the possibility of spoliation sanctions. Moreover, procedures for instituting a litigation hold should be developed.

### **B. Information to be Provided to Counsel**

Preliminary information a company should provide to counsel includes: a detailed description of computer systems used by the company, including hardware systems, primary operating systems and major software systems, including any customized software; a detailed description of how those computers are networked or connected to others outside of the company; a detailed description of how employees can network with computers from outside of the company; a detailed description of the computer systems used by employees outside of the corporate system (e.g., from home desktops, laptops and PDAs); a detailed description of the backup processes and schedules, document

**Michael T. Coutu, Esq.**

Law Offices of Sliwa & Lane

840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203

Tel.: (716) 853-2050 • Facsimile: (716) 853-2057

E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

retention and destruction schedules, organized by type of data; identify the responsible persons for each process with contact data; identify storage locations for all backup data; provide the company's document retention policy, e-mail, and internet-usage policies and litigation-hold policy, to the extent they exist; describe any monitoring or logging of employees' computer usage; and if any third parties hold or have access to the company's data, identify those third parties with full contact information.

To facilitate the collection, analysis and preservation of electronic evidence the following elements should be identified:

- The architecture and elements of the technology infrastructure, including, but not limited to, the amount and types of computers, operating systems, and software applications, including customized applications, with graphical representations, if available.
- The topology of the network environment, including, but not limited to, the physical placement of computers and their connectivity within the intranet and internet, with graphical representations, if available.
- The architecture of the electronic mail system, including, but not limited to, server and workstation software and version, lists of users, and location of email files.
- Enterprise user information applications, including, but not limited to, contact lists, calendars, to-do lists, word processing, project management and accounting.
- Internal and external personnel responsible for the management and maintenance of the technology infrastructure and all of its components with contact information.
- Information about any business activity of employees that is not backed up by the company, including the use of home machines, laptops, PDAs, etc.

**Michael T. Coutu, Esq.**

Law Offices of Sliwa & Lane

840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203

Tel.: (716) 853-2050 • Facsimile: (716) 853-2057

E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

- The names of all key players in any actual or potential lawsuit or investigation.
- The names, addresses and contact information for any third party that holds or has access to company data.
- Backup policies and procedures, including, but not limited to, hardware and software used to back up and archive information, documentation of what data is backed up, backup schedules and locations of all backup media devices.
- Computer-use policies and procedures, including, but not limited to, employee guidelines, password use, system logging, security controls, data retention, litigation holds, information sharing and acceptable internet and electronic message usage.
- The location and contents of any relevant system and event logs.

Further, the company should record each media device with a unique identifying number, then write-protect each media device. Next, each media device should be forensically duplicated to create a true mirror image. To ensure that the image is exact, it should be mathematically verified and validated by using hashing algorithms. The media devices should be scanned for viruses and spyware and the results documented. A directory structure for each media device should be created. Relevant information should then be extracted and each media device secured.

### **C. Checklist of ESI Sources**

The following is a sample checklist that can be used to ensure that all possibly relevant sources of electronically stored information are identified:

#### Electronic Information:

- Servers

**Michael T. Coutu, Esq.**

Law Offices of Sliwa & Lane

840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203

Tel.: (716) 853-2050 • Facsimile: (716) 853-2057

E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

- Mainframes
- Network file systems
- Workstations
- Laptop computers
- PDAs
- Personal home computers
- Private branch exchange
- Voicemail
- Digital printers or copiers
- Cell phones

Backup Media:

- Monthly system wide backups
- Weekly systemwide backups
- Incremental system wide backups
- Unscheduled backups
- Personal backups

Additional Media Devices:

- CD-ROMs
- DVDs
- Floppy diskettes

**Michael T. Coutu, Esq.**

Law Offices of Sliwa & Lane

840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203

Tel.: (716) 853-2050 • Facsimile: (716) 853-2057

E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

- Zip disks
- Tape archives
- Removable hard drives
- Thumb drives
- Digital camera media.

Attached as Exhibit A is a form used to identify desktop information. Exhibit B is a form for identifying key information technology personnel.

#### **D. Example**

The following fact pattern was designed to illustrate what you should do once litigation is anticipated, in light of the amended FRCP and recent New York State case law.

Assume that the plaintiff is a Housing Authority resident who slipped and fell on an allegedly icy sidewalk on March 1, 2007. As a result, she broke her ankle and was taken by ambulance to the local emergency room. The maintenance employee witnessed the ambulance taking her away and notified his manager of the incident the same day. The plaintiff alleges that she notified the Housing Authority that the sidewalk on which she allegedly fell was icy on February 2, 2007 via email and that on January 21, 2007, she phoned the maintenance department, complaining of the same icy sidewalk.

In this fact pattern, the Housing Authority can reasonably anticipate litigation as of March 1, 2007, the date of loss. Accordingly, it should immediately issue a litigation hold. Counsel should be consulted for the specifics of the litigation hold. Counsel

**Michael T. Coutu, Esq.**

Law Offices of Sliwa & Lane

840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203

Tel.: (716) 853-2050 • Facsimile: (716) 853-2057

E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

should be advised as to where e-mails, voicemails, instant messages and other electronic data is stored in case a lawsuit is commenced. Counsel should then circulate correspondence advising of the mandatory litigation hold.

The Housing Authority should issue a *written* notification to all affected employees to institute a litigation hold concerning any of the information related to the action. The litigation hold instructions should be reissued periodically and the information technology department must be made aware of the litigation hold.

The following is a sample letter that can serve as the written notification (*see* The Electronic Evidence and Discovery Handbook, 2006, American Bar Association). In the above fact pattern, this should be sent to all employees of the maintenance department, the Executive Director, all receptionists and all assistants that work for the maintenance department or Executive Director.

Re: Preservation of Electronic Data

Dear \_\_\_\_\_:

As I am sure you are aware, the advent of e-discovery has brought with it a new dimension to litigation with potentially serious consequences for the unwary. Not long ago a \$1.45 billion judgment (\$604 million compensatory, \$850 million punitive), plus ongoing interest charges in excess of \$200

**Michael T. Coutu, Esq.**  
Law Offices of Sliwa & Lane  
840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

million, was entered against Morgan Stanley. In that case, the judge took the unusual step of instructing the jury that it should assume Morgan Stanley had participated in a scheme to mislead and cover up information because it and its lawyers had consistently and deliberately violated the judge's electronic discovery orders by failing to produce internal e-mails. In another well known case, a \$29.3 million judgment was entered against UBS Warburg in favor of a former employee in the context of a sex-discrimination claim. Because of UBS's failure to preserve and produce e-mails, the court instructed the jury it could assume that any e-mails discarded by the bank after the plaintiff filed her EEOC complaint would have hurt its case. This instruction had obvious consequences given the jury's verdict. In light of these concerns, it is imperative at the outset of this litigation that you understand your obligations with respect to the preservation of electronic data and information in all its forms.

The series of reported decisions arising from the employment discrimination suit of Laura Zubulake against UBS Warburg, LLC, in the U.S. District Court, Southern District of New York, has created a set of guiding principles concerning

**Michael T. Coutu, Esq.**

Law Offices of Sliwa & Lane

840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203

Tel.: (716) 853-2050 • Facsimile: (716) 853-2057

E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

electronic discovery that must be followed in this case. In Zubulake v. UBS Warburg, LLC, 217 F.R.D. 309, 312 (S.D.N.Y. 2003) (referred to generally as "Zubulake I"), Judge Scheindlin addressed the issues of both the scope of electronic discovery and who should pay for its production. At this time there is no question, subject to any limitations set forth in the applicable procedural rules on discovery, that essentially all electronic data is potentially discoverable. This includes e-mail sent or received by any employee, other "active" information stored on servers, or information stored on backup tapes or other media that are capable of restoration, even if the information was deleted at some prior time. In the appropriate case the court will consider whether the cost of producing such information should be shifted from the party possessing the information to the party requesting the information. That determination, however, does not affect the basic obligation of every party, including business entities and all of their employees, to preserve all electronic data once the reasonable likelihood of litigation becomes apparent.

The failure to properly preserve such information can result in serious adverse consequences. In Zubulake v. UBS

**Michael T. Coutu, Esq.**  
Law Offices of Sliwa & Lane  
840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

Warburg, LLC, 220 F.R.D. 212 (S.D.N.Y. 2003) (Zubulake IV) the court addressed the obligations of the litigants. Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a "litigation hold" to ensure the preservation of relevant documents. As a general rule, that litigation hold does not apply to inaccessible backup tapes (e.g., those typically maintained solely for the purpose of disaster recovery), which may continue to be recycled on the schedule set forth in the company's policy. On the other hand, if backup tapes are accessible (i.e., actively used for information retrieval), such tapes would likely be subject to the litigation hold. If a company can identify where particular employee documents are stored on backup tapes, then the tapes storing the documents of "key players" to the existing or threatened litigation should be preserved if the information contained on those tapes is not otherwise available.

A party's obligations do not end with the implementation of a litigation hold. Counsel must oversee compliance with the litigation hold, and monitor the party's efforts to retain and produce the relevant documents. Proper communication between the lawyer and the client must ensure that all relevant

**Michael T. Coutu, Esq.**

Law Offices of Sliwa & Lane

840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203

Tel.: (716) 853-2050 • Facsimile: (716) 853-2057

E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

information, or at least all sources of relevant information, is discovered and retained on a continuing basis, and that relevant nonprivileged material is produced to the opposing party.

In Zubulake v. UBS Warburg, LLC, 2004 W.L. 1620866 (S.D.N.Y.) ("Zubulake V") the court discussed the obligation of lawyers, both in-house and outside counsel, to communicate to their clients clearly and effectively the client's obligation to preserve and timely produce all relevant electronic information, and to heed counsel's instructions on preservation on an ongoing basis. In addition, independent of the client's obligations, legal counsel have an obligation to take steps to safeguard backup tapes, request retained information from key employees, and give litigation-hold instructions to the client's key employees. Failure to follow these admonitions could result in the court finding there has been spoliation of evidence that will result in the imposition of sanctions.

To comply with counsel's obligations, once a litigation hold is in place, a party and counsel must make certain that all sources of potentially relevant information are identified and placed on hold. To do that counsel must become fully familiar with the client's document retention policies as well as the

**Michael T. Coutu, Esq.**

Law Offices of Sliwa & Lane

840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203

Tel.: (716) 853-2050 • Facsimile: (716) 853-2057

E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

client's data retention architecture. This will invariably involve speaking with information technology personnel, who can explain system-wide backup procedures and the actual (as opposed to theoretical) implementation of the firm's recycling policy. It will also involve communicating with the "key players" in the litigation in order to understand how they stored information. In Zubulake, for example, some of the UBS employees created separate computer files pertaining to the plaintiff, while others printed out relevant e-mails and retained them in hard copy only. Unless counsel interviews each employee, it is impossible to determine whether all potential sources of information have been inspected. It is not necessary that counsel review the documents at that time, only that counsel ensures that they are retained. It is not sufficient to notify all employees of a litigation hold and expect that the party will then retain and produce all relevant information. Counsel must take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched.

Once potentially relevant information is identified, there is a continuing duty to retain the information and to produce it if it is responsive to the opposing party's requests. The continuing

**Michael T. Coutu, Esq.**

Law Offices of Sliwa & Lane

840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203

Tel.: (716) 853-2050 • Facsimile: (716) 853-2057

E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

duty to supplement discovery under the Federal Rules of Civil Procedure strongly suggests that parties also have a duty to make sure that discoverable information is not lost or destroyed. To meet this obligation, counsel should issue a litigation hold at the outset of litigation. The litigation hold must be periodically reissued so new employees are aware of it and it remains fresh in the mind of all employees. Counsel must meet with the key players, explain the preservation obligation, and periodically remind them the preservation duty is still in place. Finally, all employees should be instructed to produce electronic copies of their relevant active files. Counsel must also make sure that all backup media the party is required to retain is identified and stored in a safe place. In appropriate cases counsel should take possession of the backup tapes. Alternatively, counsel can take steps to ensure the backup tapes are segregated and placed in storage.

Failure to comply with these preservation obligations could result in severe sanctions being imposed by the court including monetary penalties, the giving of an adverse inference instruction to the jury at trial, or even dismissal of certain legal claims or defenses.

**Michael T. Coutu, Esq.**

Law Offices of Sliwa & Lane

840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203

Tel.: (716) 853-2050 • Facsimile: (716) 853-2057

E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

Based on the foregoing, I would ask that you issue a written notification to all affected employees to institute a litigation hold concerning any of the information related to this action. While I understand you have discussed this with some of your employees, it is imperative that you provide everyone with written notice. In addition, you should reissue the litigation-hold instructions periodically. Please make sure you have consulted with your IT department so they are aware of the litigation hold. I would also ask that you arrange for us to have an appropriate conference with your IT supervisor so we can discuss document retention policies, backup practices, and related items. Please remind all of the key players we met at our recent meeting of their obligations in this regard. Although we did discuss their individual responsibilities to both identify and preserve any information they may have in electronic form, they need to be reminded in written form of their obligation to preserve such information. If you have any questions about these issues please contact me, so we can discuss them in detail.

## **VII. CONCLUSION**

**Michael T. Coutu, Esq.**

Law Offices of Sliwa & Lane

840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203

Tel.: (716) 853-2050 • Facsimile: (716) 853-2057

E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

Now that the new federal rules have recognized that e-discovery is important, attorneys and litigants have at least three reasons why they should learn the new rules and how to manage the discovery of electronically stored information.

First, electronically stored information or ESI is pervasive and makes up the vast majority of all discoverable material. Second, because ESI is everywhere and is, in the absence of privilege or immunity, clearly discoverable, and because it is not stored in a manner that we are all used to, such as filing cabinets, attorneys and parties must know what ESI is, where to obtain it, how to keep it, when to preserve it and how to produce it in the proper form without inadvertently waiving any privilege. Third, the cost of non-compliance, even if unintentional, significantly outweighs the cost of learning about electronically stored information and forming an efficient plan for managing e-discovery.

In summary, the new federal rules require parties in litigation to suspend the normal destruction or recycling of electronically stored information. This pertains to information stored on PDAs, laptops, computers at home and “deleted emails.”

Once litigation is reasonably anticipated, a litigation hold must be immediately imposed and counsel should be consulted to determine the details of the litigation hold. This will ensure the preservation of information that may be subject to disclosure in the event that a lawsuit is commenced and to avoid the imposition of sanctions.

**Michael T. Coutu, Esq.**  
Law Offices of Sliwa & Lane  
840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

## Exhibit A

---

### Desktop Information Form

Date \_\_\_\_\_

Case Number \_\_\_\_\_

### Computer User

Name \_\_\_\_\_

Address \_\_\_\_\_

City \_\_\_\_\_ State \_\_\_\_\_ Zip \_\_\_\_\_

Phone \_\_\_\_\_

E-Mail \_\_\_\_\_

User Name \_\_\_\_\_

Password \_\_\_\_\_

### Computer Description

Manufacturer: \_\_\_\_\_

Model: \_\_\_\_\_

Serial Number: \_\_\_\_\_

Location: \_\_\_\_\_

**Michael T. Coutu, Esq.**

Law Offices of Sliwa & Lane

840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203

Tel.: (716) 853-2050 • Facsimile: (716) 853-2057

E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

- 3 1/2-inch Floppy
- 5 1/4-inch Floppy
- 100 MB Zip
- 250 MB Zip
- CD-ROM
- CD/RW
- DVD
- Modem \_\_\_\_\_
- Firewire \_\_\_\_\_
- USB \_\_\_\_\_
- Sound \_\_\_\_\_
- NIC \_\_\_\_\_
- Tape Unit \_\_\_\_\_
- SCSI

**Michael T. Coutu, Esq.**  
Law Offices of Sliwa & Lane  
840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

Hard Disk

Evidence Number \_\_\_\_\_

- Mfg: \_\_\_\_\_
- Model: \_\_\_\_\_
- S/N \_\_\_\_\_
- Size: \_\_\_\_\_
- Interface: \_\_\_\_\_

Hard Disk

Evidence Number \_\_\_\_\_

- Mfg: \_\_\_\_\_
- Model: \_\_\_\_\_
- S/N \_\_\_\_\_
- Size: \_\_\_\_\_
- Interface: \_\_\_\_\_

BIOS Information

Access Method: \_\_\_\_\_

BIOS Date/Time: \_\_\_\_\_

Actual Date/Time: \_\_\_\_\_

Boot sequence: \_\_\_\_\_

**Michael T. Coutu, Esq.**  
 Law Offices of Sliwa & Lane  
 840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
 Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
 E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

Hard Disk 1 Geometry: \_\_\_\_\_

Hard Disk 2 Geometry: \_\_\_\_\_

Hard Disk 3 Geometry: \_\_\_\_\_

Hard Disk 4 Geometry: \_\_\_\_\_

Power Saving Features: \_\_\_\_\_

**Michael T. Coutu, Esq.**

Law Offices of Sliwa & Lane

840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203

Tel.: (716) 853-2050 • Facsimile: (716) 853-2057

E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

## Exhibit B

Title	Name and Department	Phone and e-mail
Chief Information Officer		
IT Manager		
E-mail		
Network		
Desktop/Server		
Applications/Database Manager		
Information Security		
Records Management		
Help Desk		

**Michael T. Coutu, Esq.**  
 Law Offices of Sliwa & Lane  
 840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
 Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
 E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)

Telecom		

**Michael T. Coutu, Esq.**  
Law Offices of Sliwa & Lane  
840 Main-Seneca Building • 237 Main Street • Buffalo, New York 14203  
Tel.: (716) 853-2050 • Facsimile: (716) 853-2057  
E-Mail: [mcoutu@sliva-lane.com](mailto:mcoutu@sliva-lane.com)