DOCUMENT RETENTION POLICIES AND ISSUES:
HOLD 'EM OR FOLD 'EM, BUT DON’T THROW 'EM AWAY WHEN THE FEDS ARE KNOCKING AT THE DOOR

CORPORATE, PARTNERSHIP AND BUSINESS LAW SEMINAR
University of Houston Law Foundation
June 2003

By: Ladd A. Hirsch and Jacqueline D. Novas
Table of Contents

| I. INTRODUCTION – SCOPE OF ARTICLE | ........................................... | 1 |
| II. BASIC REQUIREMENTS FOR A DOCUMENT RETENTION POLICY | ................................ | 1 |
| A. The Policy Will Vary Depending on the Type and Nature of the Business | ........ | 1 |
| B. Promoting a Reasonable Business Purpose | ................................ | 1 |
| C. Electronic Documents Must be Covered | ................................ | 2 |
| D. Basic Contents of the Document Retention Policy | ......................... | 2 |
| E. Examples of Regulatory Restrictions on Destruction of Documents | .......................... | 2 |
| III. BENEFITS OF ENFORCING A DOCUMENT RETENTION POLICY | .......... | 4 |
| A. Advantages of Having A Reasonable Document Retention Policy | ............... | 4 |
| B. Uniform and Consistent | ........................................ | 4 |
| C. Training | ............................................. | 4 |
| D. Audits | .................................................................. | 4 |
| E. Threatened Litigation or Foreseeable Investigations | ................................ | 4 |
| F. Electronic Documents and Discovery Issues | ................................ | 5 |
| 1. Introduction | ........................................ | 5 |
| 2. Electronic Search, Review and Production Software | ........ | 5 |
| 3. Electronic Mail and Other Electronic Data | ......................... | 6 |
| 4. Issues Regarding Discovery of Electronic Information | .................. | 7 |
| 5. Developing and Implementing Retention Policy for Electronic Records | ............... | 8 |
| IV. SPOLIATION: THE PERILS OF UNREASONABLE ENFORCEMENT | ........ | 8 |
| A. Definition of Spoliation | ........................................ | 8 |
| B. Duty to Preserve Documents | ......................................... | 9 |
| C. Breach of Duty | .................................................. | 10 |
| D. Prejudice to Nonspoliater | ........................................ | 10 |
| E. Sanctions for Spoliation | .................................................. | 11 |
| F. Spoliation Presumption Instruction | .................................... | 11 |
| G. A Valid Document Retention Policy Will Not Always Eliminate Adverse Consequences When Materials Have Been Destroyed | ........ | 12 |
| H. Sarbanes-Oxley Act of 2002 | ........................................ | 14 |
| 1. Introduction | ........................................ | 14 |
| 2. Title VIII – Corporate and Criminal Fraud Accountability, Section 802(a) – Criminal Penalties for Altering Documents; Tampering With a Record or Otherwise Impeding an Official Proceeding | .................. | 15 |
3. Title XI – Corporate Fraud and Accountability, Section 1102 – Tampering With a Record or Otherwise Impeding an Official Proceeding (Obstruction of Justice) ........................................ 16
4. Section 307 – New Ethical Obligations for Lawyers Representing Public Corporations .................................................. 16
5. Section 406 – Code of Ethics for Senior Financial Officers .......... 17

V. RECENT DEVELOPMENTS ................................................................. 17
   A. Walmart Stores, Inc. v. Monroe Johnson,
      Texas Supreme Court, May 22, 2003 ......................................... 17
   B. Zubulake v. UBS Warburg, 2003 WL 21087136 (S.D.N.Y. 2003) .. 18
   C. In Re CI Host, Inc., 92 S.W.3d 514 (Tex. 2002) .......................... 19
   D. Residential Funding Corporation v. DeGeorge Financial Corp.,
      306 F.3d 99 (2d Cir. 2002) ....................................................... 19
   E. Kucala Enterprises, Ltd. v. Auto Wax Co., Inc.,
      2003 WL 21230605 (N.D.Ill.), May 27, 2003 ............................ 20

VI. CONCLUSION – TIPS ON HOW TO AVOID PROBLEMS ............... 20
IMPLEMENTING AND ENFORCING
DOCUMENT RETENTION POLICIES

I. INTRODUCTION – SCOPE OF ARTICLE

In the wake of the stunning magnitude of the scandals that rocked corporate America during 2001-2002, intense focus has been brought to bear on the use of document retention policies by business entities. Specifically, politicians, lawyers, the SEC and the public have become far more interested in the details of how, when and why companies and their auditors dispose of business records. Spurred on by this new interest in document retention policies, this paper reviews the process for developing and enforcing these policies, and it also addresses both the benefits of and the potential problems that may result from the use of a document retention policy.

The first part of the paper discusses the significant purposes, of and pitfalls to avoid in implementing and enforcing a document retention (“DR”) policy, and offers practical tips on the scope and various provisions of the policy. One of the most important purposes of any DR policy is to avoid problems once a lawsuit (or other proceeding) has been threatened or filed against a company that uses a DR policy.

The final section of the paper reviews recent legal developments with an emphasis on electronic data discovery, spoliation of evidence and penalties that may be imposed against a company when it destroys documents negligently or intentionally in anticipation of (or during) a government investigation or a lawsuit. Although there are guidelines discussed in the paper, it is critical to note that there is no “one size fits all” for DR policies. Each policy must be tailored to the particular company and the specific manner in which the company conducts its business operations.

II. BASIC REQUIREMENTS FOR A DOCUMENT RETENTION POLICY

A. The Policy Will Vary Depending on the Type and Nature of the Business

The term document retention (or document management) policy “DR Policy” refers to the guidelines that are used by a company (business entity) to control the amount of time that documents are retained before they are destroyed or disposed of in some manner. In developing a DR policy, a company must address a number of issues before the policy is drafted and implemented. As noted, there is no single “model policy” that fits the needs of all types of businesses. There are different variables related to the type of business, the state in which it does business and different state and federal laws and regulations that apply to the business. There are general principles, however, that are useful for a company to consider in drafting the DR policy, regardless of the nature of the specific business.

B. Promoting a Reasonable Business Purpose

The premise that must underlie the implementation of a valid DR policy is that it will serve reasonable, legitimate business purposes. In other words, a DR policy should not be implemented
by a company solely, or even primarily, for the purpose of destroying specific documents that are, or may become, damaging if they are discovered in the company’s files. Instead, the DR policy must be supported by reasonable business concerns such as promoting efficiency, reducing costs and assisting the day to day operations of the business.

To encourage consistent implementation of a DR policy, management has to be convinced that the policy is good for the business and not just another set of burdensome guidelines created by its attorneys. Thus, the DR policy must be tailored to the particular needs of the client, otherwise there will be a risk of lax and inconsistent implementation, which will only create more problems for the client once litigation is filed or a government investigation is looming.

C. **Electronic Documents Must be Covered**

A DR policy that does not include electronic documents will almost certainly result in serious problems. A DR policy that authorizes deletion of electronic records will conserve valuable computer storage space and improve efficiency. Further, once a company becomes involved in litigation, the costs of producing electronic data can be astronomical if not well-managed. Perhaps the greatest danger from failing to provide for a system that allows for deletion of electronic records from all computers (including servers), however, is the potential for damaging e-mail(s) being produced during routine discovery. Thus, any DR policy must involve computer network personnel who will help establish the procedures required to reduce potential liability, and ensure that once a lawsuit is threatened, adequate measures are taken to prevent automatic destruction of electronic data.

D. **Basic Contents of the Document Retention Policy**

1. Define the types of documents covered, including electronic data
2. Set the retention period for each document type in compliance with applicable laws and regulations, including statutes of limitations.
3. Design procedures that will require documents to be retained if a duty arises, *e.g.*, once a lawsuit or government investigation is threatened.
4. Establish central registry and depository for retained files.
5. Develop procedures for document storage and disposition.
6. Create guidelines for implementation and enforcement of policy.
7. Establish audit procedures.
8. Secure regular updates to reflect changes in the law.

If the policy covers these elements, and the company monitors and enforces the policy, the twin goals of retaining all documents essential to conduct business, and disposing of unnecessary records will be achieved. In short, the company will dispose of wasteful, unnecessary files and in the process, rid itself of unnecessary documents that could potentially be damaging in future litigation.

E. **Examples of Regulatory Restrictions on Destruction of Documents**
Although not exhaustive, this list includes some examples of Texas and federal statutes that impose DR requirements on certain businesses:


2. **Tex. Tax Code Ann.** § 151.025 - sellers of taxable items purchased from retailers must keep records of receipts and invoices for 4 years.


6. **Internal Revenue Service.** Certain IRS regulations require the retention of tax records for at least 4 years after the date of filing the tax return or of payment of the taxes, which ever occurs later. In addition to this, records must be maintained and made available to the IRS for as long as they may be “material”. Also note that tax returns may audited 6 years after the filing date.

7. **Occupational Health and Safety Administration (OSHA).** Businesses covered by the statute are required to keep logs summarizing occupational injuries or illnesses. The retention period for these logs is five years following the end of the calendar year in which the records were generated.

8. **Employee Retirement Income Security Act (ERISA).** Any business offering retirement programs like a pension or 401(k) plan to its employees is subject to records retention regulations.

9. **Consumer Product Safety Act.** Businesses engaged in the production of certain types of consumer products are also subject to DR regulations.

10. **Environmental Records.** State and federal regulations impose retention requirements on businesses involved in hazardous waste or the production, processing, or storage of certain chemicals.
III. BENEFITS OF ENFORCING A DOCUMENT RETENTION POLICY

A. Advantages of Having A Reasonable Document Retention Policy

1. Reduction in costs: efficiency, space, volume management.
2. Avoid spoliation issues and/or obstruction of justice issues in litigation.
4. Promote uniformity in handling company records.
5. Guarantee compliance with federal and state regulations.

In order for a DR policy to be effective and to produce the anticipated benefits, however, it must go hand-in-hand with measures that ensure appropriate implementation and enforcement. A number of these are listed below.

B. Uniform and Consistent

The company must make someone specifically responsible for enforcing its DR policy. Typically, this is the general counsel, who will, in turn, delegate this responsibility to others while maintaining the ultimate authority to enforce the policy. The number of people involved in the enforcement of the retention policy depends on the company’s size. The main objective, however, is to ensure that the policy is not ignored in the press of business. A policy that is not regularly enforced may as well be non-existent.

C. Training

All employees should be provided a copy of the DR policy and periodically receive training on how it should be applied. A copy of the policy should not be given to an employee without guidelines on its application. The company should be alert to any requests for a copy of the policy, because it likely indicates a problem or issue with the application of the policy.

D. Audits

If funds permit, a company is well-advised to hire an outside party to conduct an audit on compliance with its DR policy, that results in an audit report. If the company ever becomes involved in litigation, and its DR policy is questioned, these audit reports will help establish that it was a reasonable policy and consistently enforced for legitimate business purposes. In this regard, the report should indicate the cost-savings the company achieved from disposing of unnecessary documents and electronic data.

E. Threatened Litigation or Foreseeable Investigations

Once a lawsuit (or any type of government investigation) is filed or threatened against a company, or becomes reasonably foreseeable, the company cannot destroy its documents, even if the destruction would otherwise be called for by an existing DR policy. Although the argument can be made the destruction was inadvertent, the retention policy must have an established procedure that
is designed to preserve documents once the company is placed on notice that the documents will be relevant to a threatened lawsuit or investigation.

Timing is a critical element in a court’s evaluation of whether the destruction took place in accordance with routine procedures or whether the party will be held at fault for destroying relevant business records. In *Lewy v. Remington Arms Co.*, 836 F.2d 1104 (8th Cir. 1988) the court enunciated factors that should be considered before a court imposes sanctions on a corporation for destroying documents pursuant to a DR policy: (1) whether the DR policy was reasonable considering the facts and circumstances surrounding the relevant documents; (2) the extent to which the destroyed documents were relevant to the pending or probable actions; and (3) whether the DR policy was instituted in bad faith. The court concluded that: “if the corporation knew or should have known that the documents would become material at some point in the future then such documents should have been preserved.” *Id.* at 1112.

F. Electronic Documents and Discovery Issues

1. Introduction

To develop an effective document management policy for electronic documents, in-house counsel and the company’s management must be made aware of issues that routinely arise once a lawsuit has been filed and discovery requests are served. From a trial lawyer’s perspective, a well-crafted DR policy dealing with electronic files is an essential element to effectively and efficiently manage the discovery phase of litigation. The advent of a “paperless” electronic world requires new techniques to be used in the discovery process.

The “paperless” world is one in which a much greater mass of documents is generated by more people and distributed more broadly than ever before. Multiple copies of multiple versions of documents are circulated and retained. E-mails are sent across the world instantly. We will address here some of the common evidentiary problems created by the use of email, computers, word processors, and spreadsheets.

The new age of the Internet also creates hurdles never considered 5 years ago. An example of the challenges facing companies involves their use of Internet websites and the production of information from a website. A website is not static: the information changes and is frequently updated. The ‘documents’ reflected in a website might be composed of multiple documents in separate windows. It might include various “HTML formatted pages” that actually contain three or more different pages linked together to appear as just one page. It may include a database engine that permits searches of underlying data in a report. The website might also include secure pages or intranet links that are tied to a company’s mainframe or servers.

2. Electronic Search, Review and Production Software

---

1 This section of the paper includes excerpts from a previous article co-authored by Ladd A. Hirsch, Robert Levy, Patricia Casey and Trent Stephens, “Managing Complex Litigation: Discovery In a Large Case and Common Evidence Problems”, University of Houston Law Foundation, December 2001.
When called on to produce this information, a common, traditional method is to print out all of the information to review it for privilege, and then produce it to opposing counsel in a paper form. This is often far more expensive, however, than using electronic search engines designed to support the production of electronic evidence, including e-mails, databases and document servers. This software allows for the on-line systematic and organized gathering of electronic data as well as the privilege review and preparation of a privilege log. The produced data is then part of a search engine that is used with the document database to support the evidence evaluation and analysis.

3. **Electronic Mail and Other Electronic Data**

The extensive volume and availability of documents in discovery is impacted by the common use of computerized databases in modern business. The amended Texas Rules specifically address the production of electronic data. Under Rule 196.4, litigants are required to produce electronic data that is “reasonably available,” if requested. Therefore, parties will typically request electronic mail, or “email,” which is often an incredibly fruitful source of information at trial.

Email is an efficient and cost-effective means of business communication, but involves risks and potential liability for any company. “Like ghosts from the past, these forgotten electronic blips can come back to haunt a litigant, since computer data bases are subject to civil discovery requests.” Email is inordinately susceptible to revealing “smoking gun” evidence. Its salient characteristics, particularly ease of use and informality, lead to the “immortalizing” of information that normally would never be written down or distributed in an office memo.

Email messages are just an example. A growing number of records, including insurance and accounting data, is available on computers. Multiple versions of word processing documents and spreadsheets are readily available on computers. Thus, in addition to discovery of documents in hard copy format, discovery is often requested of electronic data, which is considered crucial information. Therefore, a non-exhaustive list of the types of documents that should be subject to a DR policy (depending on the specific type of business) are: customer lists, financial records, purchase and sales reports, personnel files, original documents such as letters, memoranda, invoices, and design specifications; drafts of original documents; databases used by individuals or local area networks; computer programs reflecting a particular process, including specific information, or demonstrating proprietary methodologies; computer operation logs containing usage information; logs and text of email, including ‘trashed’ or deleted messages, message drafts, or mailing lists; electronic messaging records for messages within a specific company’s network or across a wider

---

2 See, for example, electronic discovery software developed by Kiersted Systems, Inc. of Houston, Texas, www.kiersted.com.

3 Patrick, E-Mail Data is a Ticking Time Bomb, National L J (Dec 20, 1993) at 13.


5 Jessen and Shear, Plaintiffs Take Aim at Electronic Data in Trial Discovery, Legal Times (June 20, 1994).
network, such as the Internet; manufacturer’s specifications for the computer; source codes for computer programs; voice mail transcriptions; and scheduling systems.6

4. Issues Regarding Discovery of Electronic Information

a. Gaining Control of Electronic Data. To develop a DR policy requires familiarity with the techniques for recovering and reconstructing electronic data. This includes a basic understanding of the terminology used by computer experts in the forensic area, some technical knowledge of data formats and signals, and an understanding of the various methods that are used to recover and reconstruct electronic data.7 In short, the first step to implementing an effective retention policy dealing with electronic data is to gain control of all existing computer information at the company.

b. Applicable Rules of Civil Procedure. Computer databases are subject to civil discovery requests.8 In addition to the specific provisions of the Texas Rules governing electronic discovery, the Federal Rules also permit the discovery of relevant computer-generated evidence. The 1993 revision to the Rules requires the parties to disclose the description and location of relevant data compilations early in the litigation, before a discovery request has been submitted.9

c. Costs of Production. The discovery of computer information can be costly both for the responding party, which must analyze, organize, and submit the information, and also for the party requesting discovery, because the discovery party must convert and review the information. The magnitude of this cost can be a significant consideration.10 The requesting party may be required to “pay the reasonable expenses of any extraordinary steps required to retrieve and produce the information.”11 As a result, knowing what data to request and how to respond to these requests is critical. In Rowe Entertainment v. William Morris Agency, 205 F.R.D. 421 (S.D.N.Y. 2002), the Court listed eight factors to determine whether costs of production may be allocated between the parties: (1) the specificity of the discovery requests; (2) likelihood of discovering critical information; (3) availability of information from other sources; (4) purposes for which the requested data is maintained; (5) relative benefit of obtaining the information; (6) total cost of production; (7) relative ability of each party to control costs; and (8) resources available to each party.12

6Pechette, Electronic Records Are Discoverable in Litigation, National LJ (June 27, 1994) at C8.

7There are numerous of service providers specializing in this field. Renew Data Corp., located in Austin, Texas, provided valuable ideas and information which we have incorporated in this section of our paper.


9Fed. R. Civ. P. 26 (a)


12The Rowe test for cost-shifting was recently revised in the case of Zubulake v. UBS Warburg LLC, 02 Civ. 1243, U.S.D.C. (S.D.N.Y. 2003). See discussion below in “Recent Developments” section.
In situations where the court concludes that the production of requested information without its accompanying computer analysis would result in undue hardship or burden, the court can require the producing party to use its computer system to generate the required information. The Federal Rules authorize the production of “designated documents” including “data compilations,” which clearly include electronic computer data. According to the Advisory Committee Notes, the burden is on the responding party to produce the data in a readable form, which typically means a computer printout.

5. Developing and Implementing Retention Policy for Electronic Records

a. Meet with the company’s information technology department to determine what systems are already in place to store and destroy electronic data. The information to be compiled includes, (i) the regular back-ups are made of the system, (ii) retention systems and policies, (iii) recycling and destruction of back-up tapes, (iv) existing auto-delete features in the email system, and (v) storage of copies of deleted e-mails in the server. This requires an evaluation of whether the IT department is storing too much data or destroying too much data too soon.

b. Evaluate existing statutes and regulations to determine what data must be maintained and for how long. The implementation of the retention policy must include employee education, in particular, with regards to the perils of e-mail communication. Employees must be aware of what they are required to keep on their desktops and what they are required to discard. An e-mail policy restricting the dissemination of offensive communications will also be helpful in limiting potential liability. Most importantly, if the company receives notice of potential or pending legal proceedings, company management is duty bound to inform employees and suspend the regular DR and destruction procedures.

c. One of the best enforcement procedures is to issue a well-documented periodic reminder to employees about the retention policy. Of course, copies should be retained of all reminders, internal audit records and inspections for compliance with the policy. With this documentation in hand, if there is ever a questionable destruction of records, the company will have ample evidence that its DR program is valid, reasonable, and consistently enforced.

IV. SPOLIATION: THE PERILS OF UNREASONABLE ENFORCEMENT

A. Definition of Spoliation

Spoliation is the improper destruction or alteration of evidence by a party in the context of an underlying lawsuit. Before imposing sanctions for spoliation or giving a spoliation presumption instruction, a court must inquire whether:

---


1. There was a duty to preserve the evidence at issue;
2. The alleged spoliator negligently or intentionally spoliated evidence;
3. The spoliation prejudiced the innocent party’s ability to present its case or defense.

See Trevino v. Ortega, 969 S.W.2d 950 (Tex. 1998). In a lengthy concurring opinion, Justice Baker sets forth a thorough analysis of case law on the issue of spoliation of evidence, which is summarized below along with additional cases from other jurisdictions.

B. Duty to Preserve Documents

1. A party may have a statutory, regulatory, contractual or ethical duty to preserve evidence. There may also be a common law duty to preserve evidence. Some courts have held that a party must preserve documents, tangible items, and information that are relevant to litigation or potential litigation or are reasonably calculated to lead to the discovery of admissible evidence.

2. The duty to preserve has two aspects: (a) the point at which the duty arises; and (b) the specific documents or items that the party has a duty to preserve.

a. Prelitigation duty. Being “on notice” means that point at which litigation becomes reasonably foreseeable. In National Tank v. Brotherton, 851 S.W.2d 193, 204 (Tex. 1993) the Texas Supreme Court recognized that a party may reasonably anticipate a suit being filed before the plaintiff manifests an intent to sue. Courts must look at the totality of the circumstances to determine whether reasonable person would have anticipated litigation. Offshore Pipelines, Inc. v. Schooley, 984 S.W.2d 654 (Tex. App. – Houston [1st Dist.] 1998, no pet.). Some cases that have considered this in other jurisdictions are: Blinzler v. Marriott Int’l Inc., 81 F.3d 1148, 1158-59 (1st Cir. 1996)(evidence of destruction of telephone logs admitted despite fact that they were destroyed pursuant to a policy prior to filing of case); Dillon v. Nissan Motor Co., 986 F.2d 263, 267 (8th Cir. 1993)(court had inherent power to sanction prelitigation destruction of evidence); Welsh v. United States, 844 F.2d 1239, 1241-42, 1246-48 (6th Cir. 1988); Capellupo v. FMC Corp., 126 F.R.D. 545, 551 (D.Minn. 1989); Fire Ins. Exch. v. Zenith Radio Corp., 103 Nev. 648, 747 P.2d 911, 913 (1987). Once a party is on “notice” of potential litigation a duty to preserve evidence exists. See Glover v. BIC Corp., 6 F.3d 1318, 1329 (9th Cir. 1992); McGuire v. Acufex Microsurgical, Inc., 175 F.R.D. 149, 153 (D.Mass. 1997).

15In Trevino, the Texas Supreme Court held that there is no independent cause of action for spoliation under Texas law. See also, Garcia v. Columbia Med. Ctr. of Sherman, 996 F.Supp. 605 (E.D. Tex. 1998)(applying Texas law in wrongful death action court refused to recognize independent tort of spoliation).

16Some federal statutes which have record keeping requirements include, among others: the Internal Revenue Code (IRC), Fair Labor Standards Act (FLSA), Family and Medical Leave Act (FMLA), Occupational Safety and Health Act (OSHA), Employee Retirement Income and Security Act of 1974 (ERISA) and the Americans with Disabilities Act (ADA).

17See ABA Rules of Professional Conduct, Rule 3.4(a) and DR 7-102(A)(3).
b. **Evidence which must be preserved.** There is no duty to preserve or retain every document in the company’s possession. A party has 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 or is the subject of a discovery sanction. *Wm. T. Thompson Co. v. General Nutrition Corp.*, 593 F.Supp. 1443, 1455 (C.D.Cal. 1984), aff’d, 104 F.R.D. 119 (C.D.Cal. 1985)(a potential spoliator need only do what is reasonable under the circumstances; there is no duty to take extraordinary measures to preserve evidence); *Dillon v. Nissan Motor Co.*, 986 F.2d at 267; *Capellupo v. FMC Corp.*, 126 F.R.D. at 551; *Fire Ins. Exch. v. Zenith Radio Corp.*, 747 P.2d at 914.

C. **Breach of Duty**

1. There is no need to take extraordinary measures to preserve evidence. All that is required is that the party exercise reasonable care in preserving relevant evidence. It is not clear under Texas law whether spoliation only applies to the willful or bad faith destruction of evidence or whether it also applies to the negligent destruction of evidence. Although *Trevino* and *Offshore Pipelines* state that the party should be held accountable regardless of whether the destruction is negligent or intentional, other Texas courts of appeals have held that the destruction has to be willful or in bad faith before imposing spoliation sanctions. See, *Crescendo Investments, Inc. v. Brice*, 61 S.W.3d 465, 478-79 (Tex. App. – San Antonio 2001, pet. denied); *Anderson v. Taylor Publ’g Co.*, 13 S.W.3d 56, 61 (Tex.App. – Dallas 2000, pet. denied)

a. The following cases granted or considered sanctions only for intentional or bad faith spoliation. *Caparotta v. Entergy Corp.*, 168 F.3d 754 (5th Cir. 1999); *Bashir v. Amtrak*, 119 F.3d 929, 931 (11th Cir. 1997); *Aramburu v. Boeing Co.*, 112 F.3d 1398, 1407 (10th Cir. 1997); *Vodusek v. Bayliner Marine Corp.*, 71 F.3d 148, 156 (4th Cir. 1995); *Spesco, Inc. v. General elec. Co.*, 719 F.2d 233, 239 (7th Cir. 1983).


D. **Prejudice to Nonspoliator**

Courts consider a variety of factors to determine whether a party has been prejudiced by the spoliation of evidence.

1. The relevancy of the destroyed evidence
2. Whether it is cumulative of other competent evidence still available
3. Whether the destroyed evidence supported key issues in the case.
E. Sanctions for Spoliation


1. Dismissal or default judgment against the spoliator
2. Exclusion of evidence or testimony. 18

F. Spoliation Presumption Instruction


2. There is an adverse presumption that the evidence would have been unfavorable to the spoliating party (less severe). H.E. Butt Grocery Co. v. Bruner, 530 S.W.2d 340, 344 (Tex.Civ.App.–Waco 1975, writ dism’d by agr.); Vodusek v. Bayliner Marine Corp., 71 F.3d 148, 155 (4th Cir. 1995); DeLaughter v. Lawrence County Hosp., 601 So.2d 818, 821-22 (Miss. 1992).

3. Wal-Mart Stores, Inc. v. Johnson, 2002 WL 32098152, Supreme Court of Texas, May 22, 2003. The Supreme Court reversed the Beaumont Court of Appeals which had affirmed a jury verdict for the plaintiffs. The Supreme Court held that giving the spoliation instruction was reversible error because the plaintiffs had failed to show that Wal-Mart disposed of the evidence (paper mache reindeer) after it knew or should have known that there was a substantial chance there would be litigation and that the reindeer would be material to the action. (See discussion below in “Recent Developments” section).

18 See Walton v. City of Midland, 24 S.W.3d 853 (Tex. App. – El Paso 2000, no pet.)(expert opinion and testimony could not be used as a result of expert destroying his work product).
G. A Valid Document Retention Policy Will Not Always Eliminate Adverse Consequences When Materials Have Been Destroyed

1. The existence of a valid DR policy will not always prevent an adverse result when relevant documents are destroyed. See Stevenson v. Union Pacific Railroad Company, 204 F.R.D. 425 (E.D. Arkansas 2001). In this wrongful death case, the plaintiff sought sanctions based on the railroad company’s destruction of voice dispatch tapes between a train crew and a dispatcher. Even though the tapes were destroyed pursuant to a reasonable retention policy, the court held that the defendant should have retained the tapes despite the policy.19 The court concluded that in circumstances involving death or bodily injury, the defendant’s 90-day retention period for these tapes was manifestly unreasonable and that the its adherence to this policy amounted to bad faith. Id. at 431.

2. Harris Corporation v. Ericsson Inc., 194 F.Supp.2d 533 (N.D. Texas 2002). In this patent infringement case, a best evidence issue arose regarding the admissibility of a contract missing one of its attachments. Spoliation claims were not raised, but the court commented on the plaintiff’s handling of documents: “...to say Harris’s document handling procedure has been sloppy is an understatement. This may be a result of disuniform policies between the different departments in Harris, but it is unclear...Though the court is unimpressed with this haphazard approach, it does not rise to the level of bad faith.” Id. at 541. See also, Telectron v. Overhead Door Corporation, 116 F.R.D. 107 (S.D.Fla. 1987)(absence of policy resulted in entry of default judgment for willful subversion of discovery process).

3. McGuire v. Sigma Coatings, Inc., 48 F.3d 902 (5th Cir. 1995). Sanctions were imposed on in-house counsel for defendant for destroying documents after service of requests by the plaintiffs, even though destruction was pursuant to an established DR policy. The magistrate judge’s report stated: “A worse example of bad faith is hard to imagine...Corporate in-house counsel for Fina deliberately allowed these documents to be destroyed and the court finds that severe sanctions are appropriate in this case.” The appellate court overturned the lower court’s order on personal jurisdiction grounds, but in doing so stated: “...we certainly do not intend our opinion to be construed as in any way approving of dilatory or abusive discovery tactics.” Id. at 908.

4. Ordonez v. McCurdy & Co., 984 S.W.2d 264 (Tex.App.–Houston [1st Dist.] 1998). In case involving rear-end collision the employer of the truck driver destroyed the truck driver’s log book pursuant to its normal business practice. The court found no evidence that the employer was put on notice before the destruction that the plaintiff would be making a claim. Moreover, there was no evidence that the log books were destroyed to conceal them from the plaintiff. The district court’s refusal to give the spoliation instruction was upheld. Id. at 273-74.20

---

19 For an example of an unreasonable policy, see Reingold v. Wet N’Wild Nevada, Inc., 944 P.2d 800 (Nev. 1997)(sanctions imposed for policy that allowed for destruction of accident reports before expiration of statute of limitations for personal injury actions).

20 See also Willard v. Caterpillar, Inc., 40 Cal.App.4th 892 (1995)(if company is not reasonably on notice that specific documents need to be preserved due to potential litigation, destruction pursuant to regularly followed document retention program will not lead to sanctions).
The Arthur Andersen Prosecution

a. Factual Background. It has been one year since Arthur Andersen’s conviction in June 2002 for obstruction of justice. The key events began unfolding in February 2001. At that time, Andersen was concerned with accounting practices at Enron and the possibility that Andersen’s relationship with Enron might be perceived as compromising its independence. By the Fall of 2001, Vinson & Elkins (V&E) had conducted an investigation of possible accounting improprieties in which it interviewed some Andersen partners. On October 12, 2001, on the heels of V&E’s investigation report to Enron, Andersen’s in-house counsel, Nancy Temple, sent the following internal e-mail to Michael Odom, who then forwarded it to David Duncan requesting “More Help”:

“It might be useful to consider reminding the engagement team of our documentation and retention policy. It will be helpful to make sure that we have complied with the policy. Let me know if you have any questions.”

Only four days after this e-mail, Enron disclosed a $1.2 billion drop in shareholder equity. Ten days later, on October 21, 2001, with knowledge that the SEC had begun investigating Enron, David Duncan ordered the destruction of Enron related documents. The shredding of documents did not stop until November 9, 2001, one day after Andersen received an SEC document subpoena.

b. Learning From Andersen’s Mistakes. In hindsight, Andersen’s technical compliance with its documentation and retention policy was not “helpful” or “useful,” as suggested by Nancy Temple, its in-house counsel. There are many reasons why this ill-advised e-mail backfired and helped to cause Andersen’s demise. First and foremost, if Andersen had regularly and consistently enforced its DR policy, there would have been no need to remind employees to apply the policy. Second, the timing of the e-mail reminder from Ms. Temple was devastating, because it came on the eve of a criminal investigation into Enron that Andersen should reasonably have anticipated. This e-mail triggered a massive document shredding campaign by Andersen just weeks before the SEC issued subpoenas, but after David Duncan became aware that the SEC had begun an investigation of Enron. Andersen may have argued that it was merely following an established DR policy, but it had no legitimate justification for the massive purging of documents when its in-house counsel should have reasonably anticipated that a criminal investigation of Enron was likely, and that relevant documents would be destroyed as a direct result of her e-mail reminder to the Andersen engagement team.

c. Consistent Enforcement. Andersen’s ill-timed document shredding could not pass muster as an innocent disposal of materials as part of a valid DR policy. The document destruction should have never started in light of the knowledge of the SEC investigation that David Duncan had at the time. Of the many important lessons learned from the Andersen prosecution, one of the most basic is that any DR policy must be enforced consistently for it to withstand later scrutiny. In addition, a DR policy should not be implemented when legal claims or problems are reasonably foreseeable.
H. Sarbanes-Oxley Act of 2002

1. Introduction

In the wake of the scandals involving public companies that rocked the financial markets last year, President Bush signed the Sarbanes-Oxley Act of 2002 (“the Act”)\(^{21}\) on July 30, 2002. In its broadest terms, the Act attempts to eliminate accounting fraud and restore investor confidence in the stock market. The Act contains sweeping changes to the laws affecting the directors and officers of public companies. To accomplish its goals, the Act mandates amendments to federal securities laws, including the much publicized CEO/CFO certification requirements for reports filed with the Securities Exchange Commission, increased current reporting requirements, enhanced enforcement, increased civil and criminal penalties, and increased review of periodic filings by the SEC.

This paper focuses on the Act’s amendments, which are specifically applicable to: (i) the laws that criminalize conduct that amounts to obstruction of justice and (ii) the new DR requirements for corporate audit work papers. By way of a brief summary, the Act creates a new private regulatory body, the Public Company Accounting Oversight Board (“Board”) to oversee the audit of public companies under SEC oversight. The Board will adopt audit standards and, included among these, is a new **requirement for auditors to maintain audit work papers for seven (7) years**. The obstruction of justice provisions in Title 18, U.S.C.A. ch. 73 were also amended to include a new retention requirement for audit work papers. Criminal penalties were increased to ten (10) years imprisonment for violating these statutory DR provisions. Corporate disclosure requirements now will also include a certification on a company’s code of ethics for financial officers. Finally, the SEC is required to issue regulations to establish minimum standards for the conduct of attorneys who practice before the Commission.

The contents of DR policies should be updated to comply with the new retention requirements of the Act. Moreover, the pre-Andersen technical interpretation given by corporate officers, auditors and attorneys to the application, use and enforcement of DR policies will no longer be the norm, and will not be tolerated.

2. Title VIII – Corporate and Criminal Fraud Accountability,
Section 802(a) – Criminal Penalties for Altering Documents;
Tampering With a Record or Otherwise Impeding an Official Proceeding

Title 18 U.S.C. §1519 applies to the destruction, alteration or falsification of records in federal investigations and bankruptcy proceedings. The amendments made by the Sarbanes-Oxley Act increased the penalties to 20 years imprisonment for this offense.

Title 18 U.S.C. §1520 applies to the destruction of corporate audit records. This provision is a direct result of the Arthur Andersen/Enron document shredding fiasco. The Section requires that “any accountant who conducts an audit of an issuer of securities to which section 10A(a) of the Securities Exchange Act of 1934...applies, shall maintain all audit or review work papers for a period of 5 years from the end of the fiscal period in which the audit or review was concluded.” 18 U.S.C. §1520(a)(1). Whoever “knowingly and willfully violates subsection (a)(1)...shall be fined not more than 10 years or both.” 18 U.S.C. §1520(b). In addition to the new penalties and DR requirements, subsection (c) provides that “[n]othing in this section shall be deemed to diminish or relieve any person of any other duty or obligation imposed by federal or State law or regulation to maintain, or refrain from destroying, any document.”

The SEC recently promulgated rules and regulations relating to these new retention requirements. The rules require accounting firms to retain for 7 years certain records relevant to their audits and reviews of issuers’ financial statements. Records to be retained include workpapers and other documents that form the basis of the audit or review, and memoranda, correspondence, communications, other documents and records (including electronic records), which are created, sent or received in connection with the audit or review, and contain conclusions, opinions, analyses, or financial data related to the audit or review. The rule also covers retention of records related to the audits and reviews of the financial statements of registered investment companies. These regulations will surely result in public corporation’s and auditing firms’ revisions of current DR policies. Clearly, the policy that was in effect at Arthur Andersen, which technically allowed Enron audit documents to be shredded will not pass muster under the Sarbanes-Oxley amendments.

\[22\] Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both.” (Added Pub.L. 107-204, Title VIII, §802(a), July 30, 2002, 116 Stat. 800). For the state version, see Tex.Penal Code Ann §37.09 (1999).

\[23\] Sections 103(a)(2)(A)(i) and 104(e) provide that the newly created Accounting Oversight Board (Title I of the Act) will include in its audit standards a requirement that auditors maintain work papers and other information related to an audit report sufficient to support its conclusions, for seven (7) years.

3. **Title XI – Corporate Fraud and Accountability, Section 1102 – Tampering With a Record or Otherwise Impeding an Official Proceeding (Obstruction of Justice)**

Title 18 U.S.C. §1512 (c) provides that: “whoever corruptly–(1) alters, destroys, mutilates or conceals a record, document, or other object, or attempts to do so, with the intent to impair the object’s integrity or availability for use in an official proceeding; or (2) otherwise obstructs, influences, or impedes any official proceeding, or attempts to do so, shall be fined under this title or imprisoned not more than 20 years or both.” Sarbanes-Oxley increased the penalty that applies to this offense.

The definition of obstruction of justice is found in 18 U.S.C. §1503 and it includes conduct that “corruptly...endeavors to...obstruct, or impede the due administration of justice.” The elements that the prosecution must prove are: (1) that a judicial proceeding was pending; (2) that the defendant knew that the judicial proceeding was pending; and (3) that the defendant attempted to impede that proceeding. Judicial proceedings include grand jury proceedings. These provisions may be applied to the destruction of documents in a civil proceeding between private parties. *United States v. Lundwall*, 1 F.Supp.2d 249 (S.D.N.Y. 1998).

4. **Section 307 – New Ethical Obligations for Lawyers Representing Public Corporations**

To make matters more complicated for corporate counsel, the SEC will now regulate professional conduct of attorneys practicing before the Commission. Section 307 provides that the SEC will issue rules requiring that an attorney report to the chief legal counsel or chief executive officer evidence of “a material violation of securities law or breach of fiduciary duty or similar violation” by the company or an agent acting on its behalf. If senior management does not take appropriate action, the attorney will be required to report the misconduct to the board of directors, the audit committee or a committee of non-employee board members. The SEC has recently adopted some rules to enforce Section 307.25

In essence, lawyers will now have to take affirmative action once they discover fraudulent conduct within a public company. This premise is fairly straightforward in highlighting the fact that the client is not the company CEO or CFO, but is the corporation and its shareholders. Thus, there can be no attorney-client privilege involved that would prohibit the reporting “up-the-ladder”.

It has long been a generally accepted principle that lawyers are best regulated through the state and national bar associations. The stronger role that the SEC will assume to address lawyer misconduct will bring about some controversy. Section 307 is similar to the obligations imposed

\[25\] See, 17 CFR Part 205 [Release No. 33-8185]. The SEC has prescribed minimum standards of professional conduct for attorneys appearing and practicing before the Commission in any way in the representation of issuers. The standards require an attorney to report evidence of a material violation of securities laws or breach of fiduciary duty by the issuer up-the-ladder within the company; if there is no appropriate response, the attorney will be required to take the matter to the audit committee, another committee of independent directors or the full board of directors. The “noisy withdrawal” provisions originally proposed by the SEC are still being considered.
under ABA Model Rule 1.13 which requires a lawyer to act in the best interests of the organization he represents when he becomes aware of legal wrongdoing within the organization. One of the options available under Rule 1.13 is precisely the “up-the-ladder” reporting proposed under Section 307. The SEC has not issued all the regulations to implement Section 307, in particular, the much anticipated “noisy withdrawal” provisions are still being considered.

5. Section 406 – Code of Ethics for Senior Financial Officers

Proposed rules were recently issued by the SEC under Section 406 of the Act, which requires public companies to disclose in periodic reports whether a code of ethics for senior financial officers has been adopted and the reasons for failure to do so; and any changes in a company’s code of ethics must be immediately disclosed. The proposed rules significantly expand the language of the Act.26

Specifically, although Section 406 of the Act focuses on whether a company has adopted a code of ethics applicable to its senior financial officers, the proposed rules would also apply to a company’s CEO. Thus, a company would be required to disclose whether it has adopted a written code of ethics that applies to its CEO, CFO or controller, and persons performing similar functions.

Most importantly, the rules propose to broaden the definition of the term “code of ethics” used in Section 406 of the Sarbanes-Oxley Act to include the following: (1) Honest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships; (2) avoidance of conflicts of interest, including disclosure to an appropriate person or persons identified in the code of any material transaction or relationship that reasonably could be expected to give rise to such a conflict; (3) full, fair, accurate, timely, and understandable disclosure in reports and documents that a company files with, or submits to, the Commission and in other public communications made by the company; (4) compliance with applicable governmental laws, rules and regulations; (5) the prompt internal reporting to an appropriate person or persons identified in the code of violations of the code; and (6) accountability for adherence to the code. Finally, in addition to providing the required disclosure, a company also will also have to file a copy of its ethics code as an exhibit to its annual report.

V. RECENT DEVELOPMENTS

A. Walmart Stores, Inc. v. Monroe Johnson, Texas Supreme Court, May 22, 2003

Holding: Spoliation instruction is not warranted unless there is a showing that the spoliator knew or should have known at the time the evidence was destroyed that there was a substantial chance there would be litigation and that the destroyed evidence would be material to it.

The plaintiffs in this negligence case sued Wal-Mart for injuries that Mr. Johnson allegedly sustained when a Wal-Mart employee accidentally knocked down several decorative reindeer from

---

26 See, 17 CFR Parts 228, 229 and 249 [Release No. 33-8177]. The effective date of the regulations implementing sections 406 and 407 is March 3, 2003. Companies must comply with the code of ethics and the audit committee financial expert disclosure requirements in their annual reports for fiscal years ending on or after July 15, 2003.
a high shelf onto his head and arm. At the time of the accident, Johnson claimed that he was not hurt. Six months later, however, he sued Wal-Mart. During discovery, Wal-Mart indicated that the reindeer were no longer available because they were sold or, if broken, thrown away. The only evidence of the reindeer introduced at trial was a picture that was taken during Wal-Mart’s investigation of the incident. The composition and weight of the reindeer were the object of divergent testimony at trial. Plaintiffs requested and obtained a spoliation instruction. The jury found Wal-Mart negligent and awarded $76,000 in damages to the Plaintiffs. The court of appeals affirmed.

The Supreme Court reversed and held that: (1) Wal-Mart had no duty to preserve the evidence; and (2) the spoliation instruction was harmful error. It is important to note that the Supreme Court explicitly refused to decide whether a spoliation instruction is justified when evidence is unintentionally lost or destroyed. Under the Court’s analysis, the issue of duty to preserve evidence, which is the initial inquiry for any complaint of discovery abuse, disposed of matter. The Plaintiffs did not show that Wal-Mart had disposed of the reindeer after it knew or should have known that there was a substantial chance there would be litigation and that the reindeer would be material to it. Because this showing of intentional misconduct was a necessary foundation for the submission of the spoliation instruction, the trial court abused its discretion when it submitted the spoliation instruction to the jury.


**Holding:** Defendant (responding party) is required to produce at its own expense all responsive “accessible” e-mails; and to restore and produce responsive “inaccessible” e-mails form a small sample of the back up tapes. The court modified the “cost-shifting” analysis applied in *Rowe Entm’t, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. 2002).

The Plaintiff in *Zubulake*, a gender discrimination case moved for an order to compel the production of archived e-mails. There were two questions before the court: (1) to what extent is inaccessible electronic data discoverable; and (2) who should pay for its production. The court held that the Plaintiff was entitled to the discovery of relevant e-mails that had been deleted and which existed only in back-up disks; and that consideration of cost-shifting in discovery was proper. The Defendant had argued that restoring the e-mails requested by the Plaintiff would cost approximately $175,000, exclusive of attorney time in reviewing the e-mails. The court balanced on the one hand the broad scope of discovery as prescribed under Federal Rule 26(b)(1), with the cost-consciousness of Rule 26(b)(2) on the other. The eight-factor test in *Rowe, supra*, was applied to determine whether the Plaintiff, instead of the responding party, should bear the costs of producing the e-mails.

The Court based its first holding on a broad interpretation of the term “electronic data compilations”, under Rule 34, and allowed the production of not only the electronic data that was currently in use, but also of documents that may have been deleted and now resided in back-up disks. The Defendant urged the Court to protect it from undue burden and expense and to shift the cost of production. Cost-shifting will not be considered in every case involving the discovery of electronic data, the presumption is that the responding party must bear the cost of complying with discovery requests. Cost-shifting will be considered only when electronic discovery imposes an “undue burden or expense” on the responding party. The opinion details the different media on which electronic
data is stored: (1) active, online data; (2) near-line data; (3) offline storage/archives; (4) back-up tapes; (5) erased, fragmented or damaged data. The first three categories are “accessible” while the last two are “inaccessible”. It is in the latter category that cost-shifting is to be considered.

The court modified Rowe because the factors as applied generally favored cost-shifting, instead of favoring the presumption that the responding party assumes the cost. The analysis has to be neutral and in close cases, the presumption must win. Thus, the court added new factors, eliminated some factors and determined that some factors should be given more weight than others. The seven new factors to determine whether costs of production should be shifted to requesting party, in order of importance are the following:

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.

Zubulake, 2003 WL 21087884 at p. 13. The court ultimately required the Defendant to produce at its own expense all responsive e-mails existing in its optical disks and active servers (the accessible e-mails); and to restore and produce responsive e-mails form a small sample of the back up tapes (the inaccessible e-mails).

C. In Re CI Host, Inc., 92 S.W.3d 514 (Tex. 2002)

Holding: Writ of mandamus denied. It was not an abuse of discretion for the trial court to order the production of computer back-up tapes due to the producing party’s failure to abide by the discovery rules.

This case involves a class action filed by customers of a web-host alleging breach of contract, negligence and violations of the Deceptive Trade Practices Act. The web-host had objected to the production of its computer back-up tapes on the grounds that the information contained in these tapes was protected by the Electronic Communications Privacy Act (“ECPA”). The web-host had failed to produce evidence to support its objection that all the information contained in the back-up tapes was protected under ECPA. The writ was, however, denied but the trial court was directed to consider the issuance of a protective order to cover certain confidential information contained in the back-up tapes.

D. Residential Funding Corporation v. DeGeorge Financial Corp., 306 F.3d 99 (2d Cir. 2002)

Holding: “Culpable state of mind” factor required for adverse inference instruction based on breach of discovery obligation may be satisfied by showing of mere negligence. If a party is
found to be “purposely sluggish” in producing discovery materials, this may be sufficient grounds to enter an adverse interest instruction that the materials were harmful.

The discovery dispute in this case centered on the production of e-mails contained in back-up tapes. After repeated promises to produce responsive e-mails, the plaintiff belatedly produced very few e-mails and none from the relevant period of time. On the eve of trial the plaintiff agreed to produce the back-up tapes so that a vendor retained by the Defendant could retrieve the e-mails. The plaintiff refused, however, to provide technical information that would assist the vendor in its retrieval of the e-mails. Although the plaintiff had claimed that the back-up tapes were corrupted and contained virtually no e-mails, the defendant’s vendor was able to locate 950,000 e-mails in less than 4 days. The defendant requested sanctions and an adverse inference instruction, and although the trial court denied defendant’s request, the court of appeals reversed.


Holding: Litigant that uses a wiping program such as Evidence Eliminator engages in “egregious conduct” that was wholly unreasonable; plaintiff is found at fault for not preserving evidence that it had a duty to maintain.

This case highlights the disastrous results that can befall a litigant that uses a wiping program such as Evidence Eliminator. In this patent infringement case in federal court in Illinois, the district court, in response to a discovery request by the defendant, had ordered the inspection of a computer used by the plaintiff. The defendant then hired an experienced forensic investigator to use EnCase to create a forensic image and analyze the plaintiff’s computer. On February 28th the investigator imaged the subject computer. His analysis revealed that the plaintiff had employed Evidence Eliminator on his computer between midnight and 4 AM on February 28th to delete and overwrite over 12,000 files, and that an additional 3,000 files had been deleted and overwritten three days earlier.

In addressing the propriety of the plaintiff’s use of Evidence Eliminator, the Court stated that: “Any reasonable person can deduce, if not from the name of the product itself, then by reading the website, that Evidence Eliminator is a product used to circumvent discovery. Especially telling is that the product claims to be able to defeat EnCase . . .” (emphasis added). The Court described the plaintiff’s actions as “egregious conduct” that was wholly unreasonable. As a result, the Magistrate Judge recommended to the district court that the plaintiff’s case be dismissed with prejudice, and that the plaintiff be ordered to pay the defendant’s attorney fees and costs incurred with respect to the issue of sanctions.

VI. CONCLUSION – TIPS ON HOW TO AVOID PROBLEMS

Timing is critical as it relates to DR policies and the point at which the disposal of relevant documents takes place. Therefore, even strict adherence to a valid retention policy is unlikely to justify a company’s destruction of relevant records if the destruction took place just before a lawsuit or government investigation was threatened or filed. In fact, DR on the eve of a major government
or criminal investigation may well lead to criminal charges being filed against the company and its officers. The existence of a reasonable DR policy that has been consistently followed by company personnel, however, will substantially bolster the defense to any claim of improper document destruction.

By way of a reminder, the specific steps that should be followed in developing and implementing a DR policy are set forth below:

A. Develop the Policy and Tailor It to The Needs of the Business
B. Maintain and Regularly Enforce the Policy
C. Communicate the Policy and Train All Employees to Follow it
D. Arrange for Regular Audits of the Policy, with Reports
E. Designate a Specific Person In Charge of Enforcement
F. Apply the Policy Consistently
G. Do Not Remind Employees To Comply With Retention Policy, Especially on The Eve of An Investigation or Litigation
H. Policy Needs to Have Procedure to Stop Destruction When Claim is Threatened, Lawsuit is Filed or Investigation is Announced
I. The Purpose of the Policy Should Never Be to Destroy Incriminating Material
J. Update Policy to Comply With Recent Changes in the Law