



Wednesday, October 22
11:00 am-12:30 pm

902 Proactively Managing Electronic Discovery: Challenges for Small Law Departments

Deirdre C. Brekke
Assistant General Counsel
Pactiv Corporation

Daniel R. Harper
Vice President, Corporate Counsel
Oce North America

Ronald L. Hicks
Co-Chair, Business Litigation Group
Meyer, Unkovic & Scott LLP

Kenneth A. Sprang
Chief Legal Officer
Seamless NWS, Inc.

Faculty Biographies

Deirdre C. Brekke

Deirdre C. Brekke is assistant general counsel for Pactiv Corporation located in a suburb of Chicago, Illinois. Pactiv is a leading manufacturer of food packaging and related products, including the Hefty brand line of consumer products. Her responsibilities include serving as divisional counsel to the specialty products division, managing the legal matters related to the procurement and information technology functions and handling other law department projects, including implementing an updated records retention policy and process at the company.

Prior to joining Pactiv, Ms. Brekke was with Cardean Learning Group LLC (formerly UNext.com LLC), an online education company, serving as general counsel and sole in-house attorney. Her in-house career has also included senior positions in the legal departments of Moore Corporation Limited, Sears, Roebuck & Co., and Monsanto Company.

Ms. Brekke received a BA from Emory University where she was elected to Phi Beta Kappa, and received her JD, magna cum laude, from the University of Georgia School of Law where she was inducted into Order of the Coif.

Daniel R. Harper

Dan Harper is vice president, corporate counsel for Océ-USA Holding, Inc. and is based in Chicago, Illinois. He provides general legal guidance and counsel to the North American operations of Océ N.V. a Dutch company the stock of which trades on the Amsterdam Stock Exchange. His responsibilities at Océ include counseling on commercial transactions (including sales, ERM and other vendor related), employment matters, internal investigations, litigation, corporate policy and procedure, intellectual property, software licensing, technology, and marketing.

Prior to joining Océ, Mr. Harper was senior counsel at Spiegel, Inc., where he provided legal guidance to the information technology and iMedia groups for the corporate parent as well as for Eddie Bauer, Spiegel Catalog, and Newport News subsidiaries. He also managed the Spiegel Group intellectual property portfolio, negotiated and drafted commercial transactions, managed litigation, was a member of Spiegel Group Corporate Policy Committee and was the chairman of the Spiegel Group Corporate Privacy Committee. Prior to Spiegel, Mr. Harper was in private practice with the law firm of Carey, Filter, White & Boland, a boutique general practice firm in Chicago where he divided his time between litigation and transactional work.

Mr. Harper is the past secretary of ACC's Information Technology and eCommerce Committee and is a member of the board of directors of ACC's Chicago Chapter.

He received a BA from Villanova University and is a graduate of DePaul University College of Law.

Ronald L. Hicks

Ronald L. Hicks, Jr., is a partner in the litigation section of the Pittsburgh, Pennsylvania law firm of Meyer, Unkovic & Scott, LLP. Mr. Hicks serves as a member of the firm's management committee, chair of the firm's technology committee, and co-chair of the litigation section of Meritas, an association of select independent law firms in principal cities worldwide. As a trial lawyer, Mr. Hicks provides counsel and representation in several practice areas, including business and commercial disputes, trade secret and business protection, computer and Internet law, and insurance coverage. He appears in state and federal courts throughout the Atlantic coast, and he has pursued and defended arbitration claims in locales both in and outside of Pittsburgh. He also counsels clients to adopt practices and engage in conduct that minimize their exposure to litigation.

Mr. Hicks is a frequent speaker and author on issues involving e-discovery and computer forensics, business litigation, alternative dispute resolution, and insurance coverage. Most recently, he served as a co-presenter for the National Business Institute seminars entitled "Proving Your Case with Computer Forensics" and "E-Discovery: Applying the New FRCP Changes." Also, he has presented to clients a seminar on e-mail and Internet liability titled "You've Got Mail? You've Got Liability! Workplace Privacy & Surveillance in the Era of E-mail and the Internet."

Mr. Hicks graduated with distinction from Pennsylvania State University, earning a BA. He graduated from Wake Forest University School of Law, where was elected to the Order of Barristers.

Kenneth A. Sprang

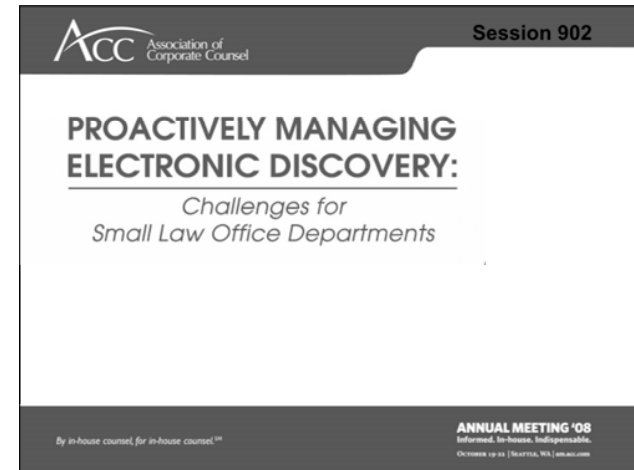
Kenneth A. Sprang is chief legal officer and secretary of Seamless NWS, Inc. in Washington, DC.

Previously, he was senior vice president, general counsel, and secretary of OnIt Digital, Inc., a start-up international interactive advertising company. Before joining OnIt, Mr. Sprang was general counsel to the Psychiatric Institute of Washington. Over the course of his career, Mr. Sprang has founded legal departments for several start-up companies, as well as working in the legal departments of Calgon Corporation, a former subsidiary of Merck & Co., Inc., and Cyclops Corporation. He also spent several years as a full-time law professor.

Mr. Sprang is a member of ACC and WMACCA, its Washington, DC chapter; the ABA and its labor section committee on the development of the law under the NLRA; and the DC and Maryland Bar Associations. He serves as pro bono general counsel to Boys To Men International and its Greater Washington and New England chapters, and he was formerly general counsel to Imago Relationships International and the Mankind Project

International. He is also a member of the board of directors of Kidsave International and volunteers as an "operations consultant" to Kidsave's DC office. Mr. Sprang is the author of several books and articles on labor and employment and alternative dispute resolution.

Mr. Sprang received his BS from the Ohio State University and an MA from the University of Michigan. He earned his law degree at Case Western Reserve University School of Law.



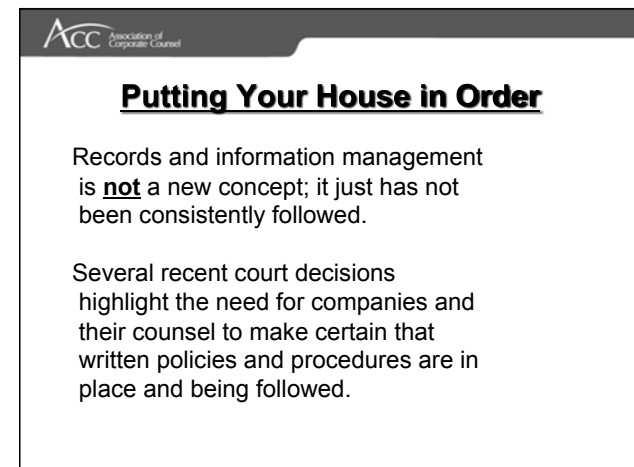
ACC Association of Corporate Counsel

Session 902

PROACTIVELY MANAGING ELECTRONIC DISCOVERY:
Challenges for Small Law Office Departments

By in-house counsel, for in-house counsel.™

ANNUAL MEETING '08
Informed. In-house. Indispensable.
October 12-13 | Seattle, WA | www.acc.com



ACC Association of Corporate Counsel

Putting Your House in Order

Records and information management is **not** a new concept; it just has not been consistently followed.

Several recent court decisions highlight the need for companies and their counsel to make certain that written policies and procedures are in place and being followed.

ACC Association of Corporate Counsel

Discussion Topics

- Creating and Implementing a Record and Information Management Program
- Litigation Readiness Programs – *Duty of management and counsel to preserve evidence, including e-data*
- Experts to assist your department – *Why, How, When, How much?*

ACC Association of Corporate Counsel

Retention Issues

- Assure proper maintenance of records
- Ensure timely and efficient disposal of records (*Zubulake IV*)
- Zubulake IV – duty to retain electronic information in accordance with your retention policies.

ACC Association of Corporate Counsel

Creating and Implementing a Record and Information Management Program

- Retention Issues
- Destruction Issues
- Record Information Management Systems
- Data Structures and Organization
- Litigation Hold Policies and Procedures

ACC Association of Corporate Counsel

Key Elements of a RIM Program

- Formal *written* policy
- Retention Schedule
- Process for execution and enforcing policy and schedule

ACC Association of Corporate Counsel

Key Retention Issues

- Permanent Record Notion
- Supporting Information
- Governing Law
- Consistency
- Duplicates, Drafts & “Extra” Sets

ACC Association of Corporate Counsel

Record/Information Management Systems

- Association for Information and Image Management (“AIIM”) (<http://www.aiim.org>)
- Association of Records Managers and Administrators (“ARMA International”) (<http://www.arma.org>)
- National Association for Information Destruction, Inc. (“NAID”) (<http://www.naidonline.org>)
- Professional Information and Records Services Management (“PRISM”) (<http://www.prismintl.org>)

ACC Association of Corporate Counsel

Destruction Issues

- “Sell ‘em” Destruction
- “Dump ‘em” Destruction
- “Hold ‘em” Destruction
- “Destroy ‘em” Destruction

ACC Association of Corporate Counsel

Data Structure and Organization

Designing a compliant records/information policy requires an understanding of your client's data structures.

Data gathering involves finding out:

1. What records or data exists?
2. What are the mediums?
3. Where are the records and data?
4. What is the operational life?
5. What is the compliance life?
6. What is the risk management life?

ACC Association of Corporate Counsel

Data Structure and Organization

Other information you should investigate:

1. When and how information is created or received?
2. How are records distributed and managed during their active life?
3. How and why duplicates are created?
4. How information is circulated vis-à-vis workflow?
5. What is the amount of hard copy and electronically stored information?

ACC Association of Corporate Counsel

Exception Management (LITIGATION)

- Exception management requires the following tasks to be performed:
 - Identify circumstances that require preservation
 - Identify records and ESI that are responsive to the preservation need
 - Inform the appropriate personnel of the litigation hold
 - Secure, segregate and preserve the records and ESI until the need for preservation is over

ACC Association of Corporate Counsel

Exception Management (LITIGATION)

- Duty to identify and “hold” all potentially relevant information arises when a party has “notice” that:
 - The records are germane to legal inquiry
 - The records may be needed for claims or defenses
 - The records may be needed to support an authorized audit

ACC Association of Corporate Counsel

Exception Management (LITIGATION)

- Failure to properly enact exception management can have serious consequences:
 - Lawsuits for spoliation of evidence
 - Adverse inference jury instruction & evidence exclusion
 - Award of attorneys' fees and costs
 - Default judgment or dismissal

ACC Association of Corporate Counsel

Socialization

- Not high on C-Level management team priority list
- Another legal spend that does not add to the bottom line
- Negative impact on bottom line
- Resource drain

ACC Association of Corporate Counsel

Measures...

- Normalize all document management and document retention policies across the company
 - centralize organization and oversight of document retention
 - identify specific people within legal, functional business units and IT
- Develop an audit protocol
- Develop a process for documenting changes to:
 - the policies
 - the compliance and audit processes relating to the policies
- Revise user policies to limit creation of redundant media collection points
- Centralize ESI recordkeeping to a limited and defined number of company systems

ACC Association of Corporate Counsel

What Measures Can You Expect to Implement?

- Collect, index and archive past and current IT policies and procedures
 - user policies
 - security policies
 - disaster recovery policies
- Collect, index and archive past and current document management and retention policies (along with schedules) – enterprise wide
- Collect, archive and document IT systems maps
- Centralize recordkeeping for documenting changes to IT systems
- Establish device inventory recordkeeping protocols to track devices (computers, portable media) issued to employees

ACC Association of Corporate Counsel

Measures...

- Eliminate storage and use of company data on non-company devices and systems
- Either:
 - ban IM, PIN and text messaging, or
 - bring all those messaging pathways into company systems that are subject to records management and retention protocols;
- Add litigation hold response protocol to document management and document retention policy
- Create a litigation response team with specifically identified representatives from the business, compliance, IT and legal departments
- Create litigation response team protocols, including form hold notices and release notices for custodians and third party data hosts

ACC Association of Corporate Counsel

Measures...

- Develop a central recordkeeping process to document distribution of litigation holds and monitor compliance with respect to all litigation holds
- Develop protocols for handling data for departing employees to ensure preservation of data subject to litigation holds
- Document and record all data destruction processes (such as laptops taken out of service, servers being upgraded)
- Analyze the feasibility of purchasing enterprise search software *i.e. EnCase Enterprise*
- Analyze the feasibility of procuring special journaling software to retain email and electronic documents of targeted custodians in ongoing litigation

ACC Association of Corporate Counsel

E-data Experts

Selecting the proper third-party is critical for the proper and efficient handling of electronically stored information.

Selecting the proper third party requires an understanding on your part as to what the needs are vis-à-vis electronically stored information: e-discovery v. computer forensics.

ACC Association of Corporate Counsel

Measures...

- Document current and prior protocols for disaster recovery
- Implement a policy requiring the sign-off of the litigation response team or legal department prior to any data destruction outside of routine DR processes
- Index all DR media on-hand and in third party storage
- Review policy and protocols with the legal department to establish minimum defensible retention period for all DR media
- Update DR protocols and establish a process for documenting all changes to DR policy
- Training

ACC Association of Corporate Counsel

E-data Experts

Other Issues to Consider:

- Certifications
- Qualifications & References
- Fees and Costs
- Look for the Truth, not the Smoking Gun

- SESSION 902 –
**PROACTIVELY MANAGING ELECTRONIC DISCOVERY:
 CHALLENGES FOR SMALL LAW OFFICE DEPARTMENTS**

Introduction

By now, you know there are new provisions in the Federal Rules of Civil Procedure that address the discovery of electronically stored information (“ESI”), which is commonly referred to as “e-discovery.” But how can you, as a member of a small law office department, determine and implement the best records/information retention and litigation hold policy for your company, so that it can efficiently and properly respond to any inevitable e-discovery request? What are the basics that you must be prepared to address? How do you protect yourself and your company from being overwhelmed by burdensome requests?

These materials will address these issues and more. The materials are divided primarily into three “Parts.” Part I will focus on the issues that you may encounter in creating and implementing a compliant record and information management program. Part II will discuss the duties that courts have imposed on management and counsel to ensure that ESI and other relevant evidence are preserved. Part III will discuss the types of “experts” that are available to assist companies with e-discovery requests and some practical advice on selecting and working with such experts. Finally, at the end of the materials are checklists and other sample documents to help you and your company manage ESI and the e-discovery process.

I. CREATING AND IMPLEMENTING A COMPLIANT RECORD AND INFORMATION MANAGEMENT PROGRAM.

Records and information management is not a new concept. For years, many companies have had record retention policies in place. However, many of those policies were ignored or not consistently followed. In the wake of such notable cases involving Arthur Andersen and KPMG, as well as the *Zubulake* decisions that are discussed in Part II of these materials, records and information management has taken on a new significance in terms of making certain that written policies and procedures are in place and being followed. Accordingly, the focus of Part I of these materials will be on creating and implementing a compliant record and information management program.

Part I of these materials is divided into five primary topic areas. The first two areas pertain to issues that arise in the retention and destruction of ESI and other relevant evidence. The next two areas highlight issues that you need to consider with respect to your company’s record and information management systems and data structures and organizations. The last area of Part I of these materials focuses on the “litigation-hold” aspects of a records and information management program.

A. Retention Issues

The retention portion of a records and information management program serves two primary purposes. First, the retention portion serves to assure maintenance of those records and information that a company must keep to meet either operational or regulatory requirements. George C. Cunningham and John C. Montaña, *The Lawyer’s Guide to Records Management and Retention*, American Bar Association, Law Practice Management Section, p. 59 (2006). For example, if a company warrants its goods for ten (10) years and the statute of limitations for

breach of warranty claims is four (4) years, then the company should keep its sales records for at least fourteen (14) years from the sale date to ensure their accessibility if litigation arises for breach of that warranty. Another example is that employee medical charts and records should be maintained for thirty (30) years after termination of employment. *See* 29 C.F.R. 1910.1020d(1).

The other purpose of the retention portion of a records and information management program is that it ensures the timely and efficient disposal of those records and information that a company does not need or should not maintain. Cunningham & Montaña, *supra.*, at p. 59. In other words, the retention portion “outlines the life cycle of records [and information], and provides for the orderly disposition of those records [and information] once a [company] no longer needs them to meet either operating or legal requirements.” *Id.*

Remember, there is no requirement that a company keep all of its records and information indefinitely. *See, e.g., Zubulake v. UBS Warburg, LLC (“Zubulake IV”),* 220 F.R.D. 212, 217 (S.D.N.Y. 2003). Instead, once a company no longer needs a record or piece of information, including without limitation ESI, to meet either operational or legal requirements (including without limitation the duty to preserve discussed in Part II of these materials), then the company is free to dispose of that record or piece of information. *Id.*

Conceptually speaking, records and information management is not complex. The documentation for a records and information management program basically involves the following three items:

- A formal written policy statement.
- A records/information retention schedule.
- Procedures for executing and enforcing the policy and schedule.

Cunningham & Montaña, *supra.*, at p. 60.

As to the policy statement, that document addresses the issues of ownership of the records and information, staff and employee duties in the context of a records and information management program, guidance over authorized copies and maintenance locales, and responsibility for program maintenance. Cunningham & Montaña, *supra.*, at p. 60. A records/information retention schedule is fundamentally a list of record types or categories, along with retention periods for those records. *Id.* The procedures for implementing the policy are simply instructions for managing the retention and disposition processes. *Id.*

Accordingly, in order to create and implement a records and information management program, a company needs to write a legally compliant policy, draft an appropriate retention schedule and then write some commonsense procedures for the retention and destruction of records and other information. Cunningham & Montaña, *supra.*, at p. 60. Of course, there will be other information, such as user lists, record logs as to the transfer of records and information into inactive storage, and documentation confirming the date and destruction of records and information, that will exist as a result of the implementation of a records and information management program. *Id.* at p. 68. However, this supporting information is ancillary to the three core documents and is generally captured in either manual or automated logs as part of the records and information management process. *Id.*

Of course, as one commentator has noted, “the devil is in the details.” Cunningham & Montaña, *supra.*, at p. 60. Considerations that go into developing retention policies may be complex and in some cases the answers are not obvious. *Id.* Political and cultural considerations may require negotiation of time periods and adjustments to policies and procedures. *Id.* Further,

actually implementing the schedule against large collections of paper and electronic documents may prove challenging. *Id.*

So, what are some of the common hurdles that a company faces when developing and implementing the records retention portion of a records and information management program? What follows are some, but not all, of the hurdles that exist when addressing the retention portion of a records and information management program, as well as possible solutions for handling such issues.

1. *The Permanent Record Notion*

One of the first issues that a company may face when addressing the record retention portion of a record and information management program is the common notion of the “permanent record.” Generally speaking, the notion arises when an objection is made that a proposed retention period is grossly inadequate because (1) the records or information have permanent enduring value and/or (2) some law requires the records and information to be kept forever. Cunningham & Montaña, *supra.*, at p. 62.

As to the first reason, the business needs of most companies do not require permanent retention since the actual business utility of the vast majority of records and information diminishes rapidly after their creation and use, and commonly drops to zero within a few years. *Id.* The reality is that though the records and information may be of supreme importance while the matter is active, at some point that matter is resolved and the usefulness of the records and information is gone. *Id.*

With respect to the second reason, in the case of general business records, the vast majority of legally mandated retention periods are well under 10 years, as are the limitations

periods for theories under which legal action involving such records and information can be brought. *Id.* Notable exceptions involve warranty claims, toxic spills, and matters involving minor children or trusts and estates. *Id.*

However, people think differently because they view their own work as important and thus should be retained forever. *Id.* at p. 63. Also, people don’t know what an appropriate retention period is and they are concerned about the penalties and consequences of disposing of records and information (particularly in light of the recent decisions that are discussed in Part III of these materials). *Id.* Hence, the “safest” course of action is to retain records and information forever, which has led to the permanent record notion. *Id.*

As counsel, your job will be to educate senior management and other employees within your company to dispel the permanent retention notion. So, how do you do that?

The most effective way to dispel the permanent record notion is to analyze the cost of maintaining the records and information. Cunningham & Montaña, *supra.*, at p. 63. Storage costs today are not cheap and will continue to grow if a record retention policy is not adopted. Once senior management and other employees within your company appreciate the cost of maintaining records and information permanently, they will understand the importance and value of the retention portion of a records and information management program.

In addition to analyzing the cost, you should discuss with senior management and other key employees the risks and utility of keeping records and information “permanently.” Cunningham & Montaña, *supra.*, at p. 63. Ask “Who will care about these records and why, in 25 or even 10 years?” It is generally revealed that most records have no value beyond 10 to 25 years and thus do not need to be retained.

Finally, if your company wants to keep records or information for a historical purpose, then a professional archivist or historian should be consulted to separate the wheat from the chaff. Cunningham & Montaña, *supra.*, at p. 64. You can locate information on the services offered by a professional archivist or historian by contacting a number of organizations, including The American Institute for Conservation of Historic & Artistic Works (<http://aic.stanford.edu/>).

2. *The Supporting Information Issue*

Another issue that a company will need to address any is the creation and maintenance of the supporting information that will be generated as part of the retention portion of a record and information management program. It should go without saying that development and maintenance of the supporting information is just as important to a records and information management program as the three core documents (*i.e.*, the written policy, retention schedules and procedures). Simply stated, the supporting information constitutes the evidence of the program's implementation. In other words, the supporting information serves as the proof that a company can use to show what its record and information management program is and that the actions taken by its employees pursuant to that program comply with both the program's requirements and with whatever law or other authority may govern the company's records retention activities. Cunningham & Montaña, *supra.*, at p. 68.

The supporting information that should be developed and maintained includes the following (which is not an exhaustive list):

- List of users;
- Logs recording the transfer of records to inactive storage;

- Audit trails documenting the movement of active records; and
- Records review and disposition details attesting to the ultimate fate of retired records.

Cunningham & Montaña, *supra.*, at p. 68.

Preservation of the supporting information is extremely important. As noted previously, this supporting information is the documentary evidence of the execution of the company's record and information management program, including without limitation the decisions made, the instructions given and the actions taken with respect to certain records and information. Cunningham & Montaña, *supra.*, at p. 68. In other words, the supporting document serves as the proof that the record and information management program is what it is and that the company's actions comply with that program. *Id.* Consequently, it is extremely important that as part of the retention portion of any record and information management program you address the questions of how and where the supporting information will be preserved.

3. *The Governing Law Issue*

One of the more time-consuming issues that a company may face with respect to the retention portion of a records and information management program is determining what law applies to the company's records and information for purposes of developing the retention schedule. Given the "Balkanized nature of U.S. law," "multiple authorities from multiple sources in multiple jurisdictions" may govern a record's retention. Cunningham & Montaña, *supra.*, at p. 86. This is especially true with regard to companies that operate in multiple jurisdictions. *Id.*

Moreover, "[r]ecords retention laws are often quite obscure." Cunningham & Montaña, *supra.*, at p. 86. Thorough research is a must, but is often hampered by varied terminology used

for the term “records,” such as “books,” “files,” “accounts” and “data.” *Id.* Further, “[t]he recordkeeping requirement in a law is often buried deep within a provision governing some substantive requirement, and may not show up on any index or other finding aid.” *Id.* As such, retention of outside counsel and utilization of resources offered by associations such as the Association of Records Managers and Administrators (“ARMA International”) (<http://www.arma.org>) are strongly recommended.

It is not a good idea to assume that federal recordkeeping requirements trump state recordkeeping requirements. Cunningham & Montaña, *supra.*, at p. 86. Also, one should not assume that the requirements across various jurisdictions and authorities within those jurisdictions are uniform. *Id.* “Federal and state authorities often exercise some form of concurrent jurisdiction, and within a jurisdiction agencies and other authorities may well promulgate requirements without regard to any other requirements affecting the same records that may already be in place.” *Id.*

Once the legal research is complete, it should be organized and incorporated into a records retention schedule, with citations to the underlying law (*i.e.*, *statute*, *regulation*, *case law*, *agency opinion*, *etc.*). Cunningham & Montaña, *supra.*, at p. 87. Moreover, it is recommended that the citations to the underlying law be displayed or linked, either individually or in groups, in the records retention schedule to the records or information that they address. *Id.* at p. 89. This process will make internal review during the development and implementation process easier, plus it will facilitate the review and updating process that should be conducted on at least an annual basis, according to some commentators. *Id.*

4. *The Consistency Issue*

Another issue that a company faces in devising and implementing the records retention portion of a records and information management program is the issue of consistency. In general, “consistency refers to the way records [and information] are treated on the [records retention] schedule, and ... the application of the schedule across all records [and information].” Cunningham & Montaña, *supra.*, at p. 68. As one commentator explained:

Conceptually, the ideal goal is to have in hand the entire record of a given transaction for the desired period of time, and then to have that entire record eliminated (and by eliminated, we mean here completely and unrecoverably obliterated) as a unified whole at the same point in time, a point identified by policy and schedule well in advance of the purge itself, so that the only remaining record of the transaction is the record of the purging itself: its date, the nature of the records destroyed, and sufficient proof that the records were purged as part of an ongoing, routine business practice.

Id. at p. 68.

Obviously, it is difficult to attain this ideal level of consistency. However, when detected by adversarial parties, erratic or inconsistent retention of records and information has led to the inference that information is being destroyed in order to hide evidence, and the courts have imposed heavy sanctions upon companies and senior management that have allowed such inconsistent behavior to occur. *See, e.g., Carlucci v. Piper Aircraft Corp.*, 102 F.R.D. 472, 486 (S.D. Fla. 1984) (the district court struck the company’s answer and entered a default as to liability because of, *inter alia*, the company’s inconsistent approach with respect to the retention and destruction of its engineering records). Thus, “a program designed and implemented with consistency in mind minimizes the likelihood of such allegations, and if they arise, it helps to defuse them.” Cunningham & Montaña, *supra.*, at p. 69.

5. *The Duplicate, Drafts and "Extra" Set Issue*

In most companies, there is more than one copy of the "official" record of a transaction. For example, duplicate copies of a record may exist in various departments or within working files, personal files, reference files or other repositories outside the official or central file or repositories. Moreover, even if the official record set or file has been disposed of in accordance with the company's record retention schedule, these duplicate, draft or extra copies of the official record may still exist and thus become discoverable and/or create a risk if they are maintained beyond the designated retention period. Cunningham & Montaña, *supra.*, at p. 92.

Organizations that have failed to recognize the issues involving duplicate, draft or extra copies have in the past been sanctioned for engaging in inconsistent record retention and destruction practices. *See, e.g., Carlucci*, 102 F.R.D. at 480-486 (default judgment as to liability entered against a company upon the company's belated disclosure of duplicate records in the flight test department of original records that had been destroyed by the engineering department). In contrast, companies that have consistently, in the course of routine business practices, executed a records retention program that consistently treat original records and copies have prevailed in court when challenged. *See, e.g., Vick v. Texas Employment Comm'n*, 514 F.2d 734, 737 (5th Cir. 1975)(trial court properly denied request for an adverse inference based on destruction of evidence where there was indication that the original and duplicate records were destroyed under routine record retention policies and procedures without bad faith).

However, it is generally not workable to implement a policy forbidding the creation of duplicate, draft or extra copies of original records. Cunningham & Montaña, *supra.*, at p. 93. The better strategy is to design the record retention portion as allowing the creation and management of such materials in a way that does not create either compliance or retention issues.

Id. For example, a company may adopt a rule that "duplicates made for the convenience of staff should be retained only so long as they are needed for their initial purpose, but no longer than the active life of the matter to which they relate[, and] [u]nder no circumstances should they be retained longer than the retention period of the official copy." *Id.*

In the end, the key to addressing duplicate, draft and extra copies is to be consistent in how they are retained and destroyed. In other words, "develop rules and follow them." Cunningham & Montaña, *supra.*, at p. 96.

B. Destruction Issues

In terms of destruction issues, you should understand that this aspect of the records and information management system is generally outsourced by most companies. Consequently, when discussing with senior management or other employees within your company on which document destruction company should be used, it is important for you, as in-house counsel, to understand how the destruction companies define "destruction."

There are primarily four definitions of destruction. First is the "Sell 'em" destruction. Cunningham & Montaña, *supra.*, at p. 220. In essence, a company seeking to have its documents destroyed is charged to have the documents picked up by the destruction company which, in turn, sells those documents to someone else for recycling. *Id.* Usually, the documents sit out in the rain or wind in loose piles or poorly secured bales before they are actually destroyed by someone else in another city, county or country, after they (or a local investigative reporter) takes a look at them. *Id.* Obviously, this destruction method is not the optimal solution for most companies.

The second definition of destruction is what is referred to as the “Dump ‘em” destruction. *Id.* Under this approach, a company seeking to have its documents destroyed is charged to have the documents picked up and delivered to a landfill, where they again sit unprotected and get blown around. *Id.* Again, this destruction method is not the best solution for most companies.

The third method of destruction is known as the “Hold ‘em” destruction. *Id.* Under this approach, a company seeking to have its documents destroyed is charged to have the documents picked up and then stored by the destruction company until there are enough records to justify the cost of having them physically destroyed. *Id.* Under this method, the stored documents may or may not be secure while they remain in the staging area waiting for destruction which may be a while, depending how long it takes the destruction company to gather a sufficient amount documents to justify the cost of the destruction process. *Id.* Depending on the company, this destruction method is not a favored solution.

The final definition of destruction is what is known as the “Destroy ‘em” destruction. *Id.* Under this approach, the destruction company arrives at the company’s facility with a large truck and grinds up the records right then and there. *Id.* The company can monitor the entire process and ensure that every file is turned into strips, confetti or powder. *Id.* Needless to say, this is the best approach for most companies.

No matter which approach is selected, it is important that the destruction of records and information be documented. Vendor’s destruction certificates are not usually specific to the necessary detail required to a client’s destruction of particular records or information. Additional documentation, preferably kept in electronic/digital format, is usually necessary. Such documentation would identify the precise records destroyed and have attached to it the vendor’s destruction certificate.

For the identification of companies involved in document destruction as well as other information regarding the document destruction process, you should review the National Association for Information Destruction, Inc.’s web site: <http://www.naidonline.org>.

C. Record/Information Management Systems

Record and information management is a set of systems, processes and tools that combine to make possible the efficient use and maintenance of all records and information within a company. Cunningham & Montaña, *supra.*, at p. 177. It also provides a framework and structure that facilitates application of the company’s records and information management policy and compliance with the records/information retention schedules. *Id.*

Automating the record and information retention functions and using technology wherever possible makes good business sense. *Id.* This is particularly true for the effective management of e-mail, word processing documents, and other electronically stored information. *Id.*

There are several national professional organizations with a records management focus. They are:

- The Association for Information and Image Management (“AIIM”) (<http://www.aiim.org>)
- The Association of Records Managers and Administrators (“ARMA International”) (<http://www.arma.org>)
- The National Association for Information Destruction, Inc. (“NAID”) (<http://www.naidonline.org>)
- The Professional Information and Records Services Management (“PRISM”) (<http://www.prismintl.org>)

A company considering automating its record and information management process should consult with a member of one of these organizations to determine which records management software would be best for it.

D. Data Structures & Organizations

Designing a compliant record and information management program requires an understanding of the company's data structures and organizations. In particular, a company needs to determine the answers to the following questions when beginning the development of a records and information program:

- What records or data exists (*i.e.*, what are all the types or kinds of records used in each practice or business function, including record titles and functional descriptions of this use)?
- What are the mediums (*i.e.*, do the records or information exist in hard copy, microform (fiche, roll, aperture card, etc.) or electronic format)?
- Where are the records and data (*i.e.*, what are the locations of the record repositories, such as hard copy file rooms, work rooms and staging areas, including electronic repositories)?
- What is the operational life of the records and data (*i.e.*, what is the period of time the record or information has some sort of real business utility and how long is a given record needed to satisfy a real business purpose)?
- What is the compliance life (*i.e.*, what is the period of time the record or information needs to be maintain to satisfy legal requirements)?
- What is the risk management life (*i.e.*, what is the period of time a record or information might be needed to satisfy the demands of a disputed resolution, litigation, audit or investigation and at what point is its continued retention starting to create a risk for the company)?

Cunningham & Montaña, *supra.*, at p. 75.

-15-

© Copyright 2008. Ronald L. Hicks, Jr. All Rights Reserved.

Other information that a company should investigate in order to design a compliant record and information management policy is the following:

- When and how information is created or received?
- How are records and information distributed and managed within the company during their active life?
- How and why are duplicates, drafts and copies created and where can they and should they end up?
- How is information circulated and does this happen according to any particular process (*a/k/a* workflow)?
- What is the amount of hard copy and electronically stored information, in terms of number of filing cabinets and boxes, server sizes, virtual servers, home offices, etc., that must be addressed during the implementation process?

Cunningham & Montaña, *supra.*, at p. 76.

To capture this information, a company may need to use different approaches, including interviews, surveys, system generated reports and inventorying of records. *Id.* No single approach is best. *Id.* The goal is to learn as much about the company's data structures, so that a compliant records and information management program that addresses all of those structures can be created and implemented.

The organization structure that a company needs to implement a compliant records and information management program will vary. At a minimum, there should be one person who is designated the records manager and that person should be a highly skilled professional who has strong communication skills, is technologically savvy, is a motivator and engages in forward thinking. Cunningham & Montaña, *supra.*, at p. 204. Additionally, the individual promoted to Information and Records Manager/Director position should be provided managerial training. *Id.*

-16-

© Copyright 2008. Ronald L. Hicks, Jr. All Rights Reserved.

at pp. 208-209. Also, the records department staff and end-users must be trained. *Id.* at pp. 210-215.

The goal of training is to inform, to train and to habituate the staff and end-users with respect to record retention and destruction policies and procedures. *Id.* Training may involve large group sessions, face-to-face training and periodic refresher training and may include you as counsel. *Id.*

Habituation is simply providing a continuous series of reminders (*i.e.*, nagging) to ensure the record and information management policy and procedures are being consistently followed. *Id.* at pp. 215-217. Companies must understand that training their employees will take time.

E. Litigation Hold Policies & Procedures

One of the most important aspects of a record and information management program is what is commonly referred to as “Exception Management.” Both common law and the *Zubulake* decisions discussed in Part II of these materials recognize a duty upon a party with notice to ensure that all sources of potentially relevant information are identified and placed “on hold.” *See, infra.*, Part II.A-C. Consequently, just as a record and information management program identifies and deals with records for retention and disposition, so too must it identify and deal consistently with documents that are to be temporarily excluded from the disposition process. Cunningham & Montaña, *supra.*, at p. 69.

Although discussed in greater detail in Part II.B of these materials, the duty to place a hold on records and information that would normally be subject to destruction under a records and information management program arises when reasonable notice exists that:

- The records are germane to a lawsuit, regulatory investigation or similar legal inquiry;

-17-

© Copyright 2008. Ronald L. Hicks, Jr. All Rights Reserved.

- The records may be needed to preserve or advance the rights of a client or ex-client; or
- The records may be needed to support an authorized audit.

Cunningham & Montaña, *supra.*, at pp. 69-70.

Failure to segregate and maintain records and information when on notice of any of the above circumstances may have very serious consequences for a company and possibly senior management. *See, infra.*, Part II.C-D. Therefore, the program must include mechanisms to perform the following tasks:

- Identify circumstances that may require the preservation of records and ESI otherwise scheduled for destruction;
- Identify the records and ESI that are responsive to the need identified;
- Quickly and accurately inform the appropriate personnel of the identity of the records and ESI involved and of the need to preserve them; and
- Secure, segregate and preserve those records and ESI until such time as the circumstances requiring their retention have ceased.

Cunningham & Montaña, *supra.*, at p. 70.

Failure to properly execute what is commonly referred to as a “litigation or legal hold” can result in severe penalties. *See, infra.*, Part II.C-D. However, such penalties should not serve as an excuse to not create and implement a records and information management program. Cunningham & Montaña, *supra.*, at p. 70. Instead, a properly developed and implemented exception management portion of a records and information management program should not interfere with the overall program and should help facilitate it by allowing irrelevant records and information to be destroyed in accordance with normal business operations. *Id.* The key is that for the exception management portion to work properly, the procedures for accomplishing the

-18-

© Copyright 2008. Ronald L. Hicks, Jr. All Rights Reserved.

exception to a company's record and information management program must be clear and thorough, effectively communicated to everyone in the company, and consistently followed and monitored. *Id.* at 101.

II. PRESERVING ELECTRONICALLY STORED INFORMATION UNDER THE NEW FEDERAL RULES OF CIVIL PROCEDURE

Even if you have established a records and information management program for your company, that program will not protect your company or its employees from sanctions if the program's policy and procedures are not followed when litigation or an investigation becomes evident. Thus, while a properly drafted and implemented records and information management program will lower the possibility that your company and its employees will be found to have destroyed evidence in bad faith, if the program's policy and procedures are blindly administered, inadequately distributed to employees or fail to take into account the effects of litigation or an investigation, your company and its employees may be subject to sanctions. A cursory review of recent cases illustrates that courts are increasingly requiring management and counsel (both in-house and outside) to ensure that ESI, as well paper documents and other relevant evidence, are preserved when litigation or an investigation is filed, threatened or reasonably foreseeable.

This section of these materials will discuss the duties that courts have been imposing on management and counsel to ensure that ESI and other relevant evidence are preserved. Because retaining evidence is important to avoid sanctions, this section of the materials will address first the questions of what is the duty to preserve evidence and when does that duty arise. Then, the materials will point out some of the consequences for failing to preserve ESI and other relevant evidence. Lastly, this section of the materials will discuss certain illustrative cases that

emphasize the importance of evidence preservation and the need for management and counsel to become personally involved in ensuring that ESI and other relevant evidence are preserved.

A. What Is The Duty To Preserve Evidence?

Generally speaking, before sanctions can be imposed, the party against whom sanctions are sought must have had a duty to preserve evidence. Drew D. Dropkin, *Linking the Culpability and Circumstantial Evidence Requirements for the Spoliation Inference*, 51 Duke L.J. 1803, 1807-08 (2002). Several courts have relied upon statutes, regulations and rules governing party and attorney conduct to hold that a duty to preserve evidence exists. *See, e.g., Byrnie v. Town of Cromwell Bd. of Educ.*, 243 F.3d 93, 108-109 (2d Cir. 2001) ("We agree that, under some circumstances, ... a regulation can create the requisite obligation to retain records, even if litigation involving the records is not reasonably foreseeable."); *Latimore v. Citibank Fed. Sav. Bank*, 151 F.3d 712, 716 (7th Cir. 1998) ("The violation of a record[-]retention regulation creates a presumption that the missing record contained evidence adverse to the violator."); *Favors v. Fisher*, 13 F.3d 1235, 1239 (8th Cir. 1994) (because employer violated record retention regulation, plaintiff "was entitled to the benefit of a presumption that the destroyed documents would have bolstered her case"); *Hicks v. Gates Rubber Co.*, 833 F.2d 1406, 1419 (10th Cir. 1987) (same). *See also* Steffen Nolte, *The Spoliation Tort: An Approach to Underlying Principles*, 26 St. Mary's L.J. 351, 368-69 (1995) (collecting cases announcing a tort cause of action for spoliation based on violation of record-retention regulations).

The Model Rules of Professional Conduct address spoliation in Rule 3.4: "A lawyer shall not unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value." Model Rules of Professional

Conduct, Rule 3.4(a) (2008). The Committee Comment to Rule 3.4 provides the policy behind the rule:

Fair competition in the adversary system is secured by prohibitions against destruction or concealment of evidence, improperly influencing witnesses, obstructive tactics in discovery procedure, and the like. ... Documents and other items of evidence are often essential to establish a claim or defense. Subject to evidentiary privileges, the right of an opposing party ... to obtain evidence through discovery or subpoena is an important procedural right. The exercise of that right can be frustrated if relevant material is altered, concealed or destroyed. Applicable law in many jurisdictions makes it an offense to destroy material for purpose of impairing its availability in a pending proceeding *or one whose commencement can be foreseen.*

Id. at 3.4(a) cmt. 1-2 (emphasis added).

Additionally, a duty to preserve evidence may arise if the party voluntarily assumed a duty to preserve a document. *See Allis-Chalmers Corp. Prod. Liab. Trust v. Liberty Mut. Ins. Co.*, 702 A.2d 1336 (N.J. Super. Ct. App. Div. 1997) (holding that absent an agreement, contract or voluntary assumption on the part of one party to preserve, there is no duty for an individual who is not the owner of property to preserve the property). For instance, a party may voluntarily assume a duty to preserve evidence where a formal document retention policy creates such a duty. *See Dropkin, supra.*, 51 Duke L.J. at 1808.

Further, common law may provide a basis for a duty to preserve evidence. For example, it is generally recognized that a "duty [to preserve evidence] arises when litigation is filed, threatened, or reasonably foreseeable." *Id.* *See also Zubulake v. UBS Warburg, LLC* ("Zubulake IV"), 220 F.R.D. 212 (S.D.N.Y. 2003)(Under common law, the duty to preserve documents and information "arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation.") This duty

commonly arises when a party receives a demand letter or summons and complaint. *See Mosaid Techs. Inc. v. Samsung Elecs. Co.*, 348 F. Supp. 2d 332, 336 (D.N.J. 2004). However, the obligation to preserve evidence may arise even earlier if a party has sufficient notice or information that a credible threat of future litigation exists. *See, e.g., Kronisch v. United States*, 150 F.3d 112, 126 (2d Cir. 1998); *Henkel Corp. v. Polyglass USA, Inc.*, 194 F.R.D. 454, 456 (E.D.N.Y. 2000). While a party is not permitted to destroy potential evidence after receiving sufficient notice of impending litigation, the duty to preserve relevant documents requires more than a mere possibility of litigation. *See Hynix Semiconductor Inc. v. Rambus, Inc.*, 2006 U.S. Dist. LEXIS 30690, 2006 WL 565893, *21 (N.D. Cal. 2006). Ultimately, the facts of each case decide when a party's duty to preserve exists. *See Cache La Poudre Feeds, LLC v. Land O'Lakes Farmland Feed, LLC*, Civil Action No. 04-cv-00329-WYD-CBS, 2007 U.S. Dist. LEXIS 15277, at *24 (D. Colo. Mar. 2, 2007).

The duty to preserve evidence applies not only to the parties involved, but also to non-parties. Laurie Kindel and Kai Richter, *Spoilation of Evidence: Will the New Millennium See a Further Expansion of Sanctions for the Improper Destruction of Evidence?*, 27 Wm. Mitchell L. Rev. 687, 689 (2000). "Whether or not the party is a litigant or potential litigant greatly impacts the breadth of the duty and when the duty arises. Courts are far more likely to impose a duty to preserve evidence on persons and entities who are or may become litigants." *Id.*

B. When Does The Duty To Preserve Evidence Attach?

Courts universally agree that when a complaint has been filed and served upon a named defendant, that party is under a duty to preserve all documents that are relevant to the claims and defenses in that litigation. *See, e.g., Danis v. USN Communications*, 2000 WL 1694325, at *5 (N.D. Ill. Oct. 23, 2000) ("As of November 12, 1998, the date that this litigation commenced,

USN had a duty to preserve documents and other information that might be discoverable in the litigation”). However, courts have also ruled that “[t]he duty to preserve material evidence arises not only during litigation but also extends to that period before the litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation.” *Silvestri v. General Motors Corp.*, 271 F.3d 583, 591 (4th Cir. 2001).

“When a lawsuit has not been filed and there is no specific statutory or other legal duty between the parties to preserve evidence, the question becomes whether it is ‘reasonably foreseeable’ that a lawsuit will ensue and that the evidence will be discoverable in connection with that suit.” Jeffrey S. Kinsler and Anne R. Keyes MacIver, *Demystifying Spoliation of Evidence*, 34 Tort & Ins. L.J. 761, 761, n. 10 (1999). For example, it may be reasonably foreseeable for a party to be on notice of anticipated litigation through correspondence between the parties’ counsel before the complaint is filed. *See, e.g., William T. Thompson Co. v. General Nutrition Corp.*, 593 F. Supp. 1443, 1446 (C.D. Cal. 1984) (“Notice was provided by the pre-litigation correspondence between counsel for the parties”). Hence, it is important to have an understanding of what constitutes “reasonably foreseeable” conduct for purposes of the duty to preserve evidence.

“In making determinations of foreseeability, courts recognize the unique problems faced by large organizations and have criticized unreasonably expansive duties to preserve evidence as immensely burdensome.” Kinsler & Keyes MacIver, *supra.*, 34 Tort & Ins. L.J. at 772. Consequently, “where litigation is merely possible, but not ‘reasonably foreseeable’, routine document disposal is highly unlikely to result in spoliation sanctions.” *Id.* To date, the United States Supreme Court has not articulated when litigation is “reasonably foreseeable.” Hence, the

federal courts have been left to address the issue on their own. What follows is a highlight of some of the federal appellate court decisions on when the duty to preserve evidence exists.

1. Second Circuit

The Second Circuit has held the duty to preserve evidence arises “when the party has notice that the evidence is relevant to litigation - most commonly when suit has already been filed, providing the party responsible for the destruction with express notice, *but also on occasion in other circumstances, as for example when a party should have known that the evidence may be relevant to future litigation.*” *Kronisch v. United States*, 150 F.3d 112, 126 (2d Cir. 1998). In *Kronisch*, the defendants, who were CIA employees, argued they destroyed documents relating to a CIA-sponsored study on the effects of lysergic acid diethylamide (LSD) in order to preserve the confidentiality of the test subjects and because they feared the documents would be “misunderstood.” *Id.* at 127. The Second Circuit found that the defendants’ “own expressed fear that the documents might be ‘misunderstood’ could be interpreted in a number of ways, including as a fear that the documents would become the subject of litigation.” *Id.* Thus, the Second Circuit held there was enough evidence for a jury to decide that the defendants destroyed the documents because they believed the documents would be used against them in a future lawsuit. *Id.* As the Second Circuit explained:

The district court properly rejected defendants’ argument that an adverse inference was not warranted because at the time the MKULTRA documents were destroyed in 1973 no litigation, administrative action, or congressional investigation had commenced, and because Helms’s and Gottlieb’s reasons for destroying the evidence allegedly had nothing to do with the fear of future litigation. *See Kronisch III*, 1997 WL 907994, at *21. Although defendants claimed that the documents were destroyed to preserve the confidential identities of outside participants in the MKULTRA program, to prevent incomplete documents from being misunderstood, and to prevent paper overflow, the district court concluded that “it is somewhat hard to believe that both

Gottlieb and Helms ... were concerned only with the effect of disclosure on other persons connected to the drug program, and not with the possible consequences to themselves or to the CIA." *Kronisch III*, 1997 WL 907994, at *22. Moreover, the district court observed, Gottlieb's own expressed fear that the documents might be "misunderstood" could be interpreted in a number of ways, including as a fear that the documents would become the subject of litigation. *See id.* At the very least, the district court could not rule out the possibility that a reasonable jury would find that Helms and Gottlieb feared the prospect of litigation against them individually, and that this prospect may have played a role in their decision to order the destruction of MKULTRA files. ... Defendants do not challenge this sound approach on appeal.

Kronisch, 150 F.3d at 127.

Finally, the Second Circuit has held that "under some circumstances," a regulation that requires the retention of evidence for a period of time can create the requisite obligation to retain records, "even if litigation involving the records is not reasonably foreseeable." *Byrnie*, 243 F.3d at 108-109. However, for such a duty to attach, "the party seeking the inference must be a member of the general class of persons that the regulatory agency sought to protect in promulgating the rule." *Id.* at 109. As the Second Circuit has explained:

For example, violation of a rule that records be retained for securities disclosure purposes would not create a duty to preserve covered records for use in a subsequent employment discrimination suit. On the other hand, where, as here, a party has violated an EEOC record-retention regulation, a violation of that regulation can amount to a breach of duty necessary to justify a spoliation inference in an employment discrimination action. In such a case we can be confident that the responsible agency had in mind persons in the plaintiff's position and accordingly that our finding a duty to preserve documents in such circumstances will advance the goals of the rule.

Id. (citations omitted).

2. Fourth Circuit

Like the Second Circuit, the Fourth Circuit has held that "[t]he duty to preserve material evidence arises not only during litigation but also *extends to that period before the litigation* when a party reasonably should know that the evidence may be relevant to anticipated litigation." *Silvestri*, 271 F.3d at 591 (emphasis added). In *Silvestri*, the plaintiff alleged his injuries from a car accident were enhanced by a defective air bag that failed to deploy when he crashed the car into a utility pole. *Id.* at 585. The district court dismissed the plaintiff's lawsuit, holding that the plaintiff had destroyed evidence because the defendant manufacturer did not have notice of the plaintiff's claim and an opportunity to inspect the vehicle before it was repaired. *Id.* On appeal, the plaintiff argued that he did not have a duty to preserve the vehicle because he did not own the car and any act of spoliation was caused by his attorney and should not be imputed to him. *Id.* at 598. The Fourth Circuit disagreed, stating, the "duty to preserve material evidence arises not only during litigation but also extends to that period before the litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation." *Id.* at 591. Because the plaintiff had anticipated filing a lawsuit against the defendant manufacturer and knew the vehicle was relevant evidence in that suit, the plaintiff had a duty to notify the defendant of his claim and allow the manufacturer access to the vehicle before it was repaired. *Id.* at 592. In response to the plaintiff's argument that he did not own the car, and, therefore, could not preserve it, the court stated that "[i]f a party cannot fulfill this duty to preserve because he does not own or control the evidence, he still has an obligation to give the opposing party notice of access to the evidence or of the possible destruction of the evidence if the party anticipates litigation involving that evidence." *Id.* at 591.

3. Sixth Circuit

Relying upon Michigan state law, the Sixth Circuit has ruled that there is a duty to preserve evidence before litigation has commenced, where the party “knows or should know [the evidence] is relevant before litigation is commenced.” See *Beck v. Haik*, 377 F.3d 624, 641 (6th Cir. 2004). In *Beck*, the plaintiff sued various city and county officials after the plaintiff’s son drowned. *Id.* at 629. At trial, the plaintiff argued the defendant despoiled evidence because it failed to preserve the dispatch tapes of the events that occurred on the night of the drowning. *Id.* at 640. The district court held there was inadequate evidence of spoliation because the written request for the information was filed with the sheriff’s office and not with the dispatch office. *Id.* at 641. The Sixth Circuit reversed, stating that even though the written request was filed with the wrong office, the dispatch office was already on notice of the need to preserve the dispatch tape because the Coast Guard had made a verbal request for the tape. *Id.* at 640-41. Thus, there was sufficient evidence for the plaintiff to present its spoliation evidence to the jury. *Id.*

4. Eighth Circuit

The Eighth Circuit is one of the few federal appellate courts that have address the question of what constitutes “reasonably foreseeable” notice in conjunction with the destruction of business records pursuant to a company’s document retention policy. In *Lewy v. Remington Arms Co.*, 836 F.2d 1104 (8th Cir. 1988), the Eighth Circuit held that litigation is “reasonably foreseeable” if a company has received complaints or has been sued in matters similar to the subject of the current lawsuit. *Lewy*, 836 F.2d at 1112. In *Lewy*, the plaintiff brought a products liability claim against the defendant rifle manufacturer, Remington Arms Company, because the subject rifle discharged after the safety was moved to the fire position. *Id.* at 1105. After the jury returned a verdict for the plaintiff, Remington Arms appealed, arguing in part that the

district court erred in allowing the jury to draw an adverse inference from the company’s inability to produce records that had been destroyed pursuant to the company’s document retention policy. *Id.* at 1111. The records that had been destroyed concerned complaints about the subject rifle and certain rifle examination reports. *Id.*

While being unable to decide whether the trial court had committed error based on the record before it, the Eighth Circuit stated that if, on remand, the trial court was asked again to instruct the jury regarding failure to produce evidence, the trial court should consider “whether [the company’s] record retention policy is reasonable considering the facts and circumstances surrounding the relevant documents.” *Id.* at 1112. In particular, the Eighth Circuit instructed the trial court to “determine whether a three year retention policy is reasonable given the particular document.” *Id.* According to the Eighth Circuit, “[a] three year retention policy may be sufficient for documents such as appointment books or telephone messages, but inadequate for documents such as customer complaints.” *Id.*

Further, the Eighth Circuit noted that the trial court should consider was “whether lawsuits concerning the complaint or related complaints have been filed, the frequency of such complaints, and the magnitude of the complaints.” *Id.*

Finally, the Eighth Circuit ruled that the trial court should determine whether the company’s document retention policy was instituted in bad faith. *Id.* As to this factor, the Eighth Circuit stated as follows:

In cases where a document retention policy is instituted in order to limit damaging evidence available to potential plaintiffs, it may be proper to give an instruction similar to the one requested by the Lewys. Similarly, even if the court finds the policy to be reasonable given the nature of the documents subject to the policy, the court may find that under the particular circumstances certain documents should have been retained notwithstanding the policy.

For example, *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*. Thus, a corporation cannot blindly destroy documents and expect to be shielded by a seemingly innocuous document retention policy.

Id. (emphasis added; citations omitted).

Sixteen years after its decision in *Lewy*, the Eighth Circuit explained that despite the fact that the “knew or should have known” language is commonly understood to be a negligence standard, “such a standard, standing alone, would be inconsistent with the bad faith consideration and the intentional destruction required to impose an adverse inference for the prelitigation destruction of documents.” *Stevenson v. Union Pacific R.*, 354 F.3d 739, 746-47 (8th Cir. 2004). According to the Eighth Circuit, it has “never approved of giving an adverse inference instruction on the basis of prelitigation destruction of evidence through a routine document retention policy on the basis of negligence alone.” *Stevenson*, 354 F.3d at 747. Accordingly, “[w]here a routine document retention policy has been followed in this context, ... there must be some indication of an intent to destroy the evidence for the purpose of obstructing or suppressing the truth in order to impose the sanction of an adverse inference instruction.” *Id.* Cf. *Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99, 107 (2d Cir. 2002) (a “culpable state of mind” for purposes of a spoliation inference includes ordinary negligence).

C. **What Happens If Evidence Is Not Preserved?**

To date, the United States Supreme Court has not addressed the standards for preservation and seizure of ESI and the applicable sanctions where such evidence has been destroyed or lost. The cases that have been recognized as setting the benchmark standards for modern discovery and evidence preservation issues are the series of *Zubulake* decisions out of the Southern District of New York. See *Zubulake v. UBS Warburg, LLC (“Zubulake I”)*, 217

F.R.D. 309 (S.D.N.Y. 2003); *Zubulake v. UBS Warburg, LLC (“Zubulake II”)*, 230 F.R.D. 290 (S.D.N.Y. 2003); *Zubulake v. UBS Warburg, LLC (“Zubulake III”)*, 216 F.R.D. 280 (S.D.N.Y. 2003); *Zubulake v. UBS Warburg, LLC (“Zubulake IV”)*, 220 F.R.D. 212 (S.D.N.Y. 2003); *Zubulake v. UBS Warburg, LLC (“Zubulake V”)*, 229 F.R.D. 422 (S.D.N.Y. 2004); and *Zubulake v. UBS Warburg, LLC (“Zubulake VI”)*, 382 F. Supp.2d 536 (S.D.N.Y. 2005). Accordingly, any discussion regarding what happens if ESI and other relevant evidence are not preserved must involve an examination of the principles outlined in *Zubulake*.

According to *Zubulake IV*, spoliation is “the destruction or significant alteration of evidence, or the failure to preserve property for another’s use as evidence in pending or reasonably foreseeable litigation.” *Zubulake IV*, 220 F.R.D. at 216. See also *Allstate Ins. Co. v. Hamilton Beach/Proctor Silex, Inc.*, 473 F.3d 450, 457 (2d Cir. 2007) (quoting *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir. 1999)). The determination of a proper sanction for spoliation of evidence is confined to the sound discretion of the trial judge, and must be made on a “case-by-case” basis. *Zubulake IV*, 220 F.R.D. at 216. Further, the trial court’s authority to sanction litigants for spoliation arises both under the Federal Rules of Civil Procedure and the court’s inherent powers. *Id.*

According to *Zubulake IV*, a party, upon recognizing the threat of litigation, need not preserve “every shred of paper, every e-mail or electronic document, and every backup tape.” *Zubulake IV*, 220 F.R.D. 212 at 217. Instead, the duty to preserve extends to only those documents or tangible things made by individuals “likely to have discoverable information that the disclosing party may use to support its claims or defenses.” *Id.* at 218. The duty also extends to documents prepared for those individuals and to information that is relevant to the claims and defenses of any party, or which is “relevant to the subject matter involved in the action.” *Id.*

Thus, the duty to preserve extends only to those employees likely to have relevant information, *i.e.* the "key players" in the litigation. *Id.*

In sum, the scope of a party's preservation obligations has been described as follows:

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), then such tapes would likely be subject to the litigation hold.

Zubulake IV, 220 F.R.D. at 218.

According to *Zubulake V*, after a "litigation hold" is in place, "a party and [its] counsel must make certain that all sources of potentially relevant information are identified and placed 'on hold,' to the extent required in *Zubulake IV*." *Zubulake V*, 229 F.R.D. at 432. Furthermore, it is counsel who "must oversee compliance with the litigation hold, monitoring the party's efforts to retain and produce the relevant documents." *Id.* As the court in *Zubulake V* explained: "Proper communication between a party and [its] lawyer will ensure (1) that all relevant information (or at least all sources of relevant information) is discovered, (2) that relevant information is retained on a continuing basis; and (3) that relevant non-privileged material is produced to the opposing party." *Id.*

In *Zubulake V*, the court laid out a list of guidelines that counsel should follow in order to avoid sanctions for spoliation of ESI. *Zubulake V*, 229 F.R.D. at 432-436. Those guidelines can be summarized as follows:

- Counsel must become fully familiar with the client's document retention policies and data retention and computing infrastructure, speaking with the client's key information technology personnel about such policies and systems.
- Counsel should talk with the "key players" in the litigation (*i.e.*, the people identified in a party's initial disclosure and any subsequent supplementation thereto), inquiring as to how and where they store their information or data and advising them of their preservation of evidence obligations.
- Counsel must affirmatively monitor compliance with the "litigation hold" and take reasonable steps to see that all sources of discoverable information are identified, searched and located.
- Counsel must ensure that the "litigation hold" is implemented at the outset of litigation or whenever litigation is reasonably anticipated, and periodically reissue the notice so that new employees are aware of it, and so that it is fresh in the minds of all employees.
- Counsel should periodically remind the "key players" in the litigation that the "litigation hold" remains in place and of the preservation of evidence obligations.
- Counsel should instruct all employees to produce electronic copies of their relevant active files and ensure that relevant backup tapes or other archival media are safely stored and segregated from other such media.

Zubulake V, 229 F.R.D. at 432-436.

The *Zubulake V* guidelines are not meant to be onerous. Instead, the actions of counsel "must be reasonable." *Zubulake V*, 229 F.R.D. at 433. Counsel is not obliged to monitor his or her client like a parent watching a child. *Id.* However, because "counsel is more conscious of the contours of the preservation obligation; a party cannot reasonably be trusted to receive the 'litigation hold' instruction once and to fully comply with it without the active supervision of counsel." *Id.*

According to *Zubulake V*, three elements are necessary to support a claim of spoliation. *Zubulake V*, 229 F.R.D. at 430 (*citing Byrne*, 243 F.3d at 107-12). Those elements are: "(1) that

the party having control over the evidence had an obligation to preserve it at the time it was destroyed; (2) that the records were destroyed with a 'culpable state of mind'[:]; and (3) that the destroyed evidence was 'relevant' to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense." *Id.*

A variety of sanctions may be imposed for a failure to preserve ESI and other relevant evidence when litigation is reasonably foreseeable. As the *Zubulake* decisions acknowledge, courts have an inherent power to impose sanctions, *see Zubulake IV*, 220 F.R.D. at 216, "but the power is limited to that necessary to redress conduct which abuses the judicial process." *Thompson v. U.S. Dep't of Hous. & Urban Dev.*, 219 F.R.D. 93, 100 (D.Md. 2003).

The most common sanction is the adverse inference instruction. When evidence that is relevant to an issue is destroyed, the court may instruct the jury that it is permitted to infer that "the party who obliterated the evidence did so out of a realization that the contents were unfavorable." *Blinzler v. Marriott Int'l, Inc.*, 81 F.3d 1148, 1158 (1st Cir. 1996). Generally, the following four factors are considered before a trial court will give an adverse inference jury instruction:

- (1) the party's degree of control, ownership, possession or authority over the destroyed evidence;
- (2) the amount of prejudice suffered by the opposing party as a result of the missing or destroyed evidence and whether such prejudice was substantial;
- (3) the reasonableness of anticipating that the evidence would be needed for litigation; and
- (4) if the party controlled, owned, possessed or had authority over the evidence, the party's degree of fault in causing the destruction of the evidence.

Hannah v. Heeter, 584 S.E.2d 560, 567 (W.Va. App. 2003).

Additionally, at least one court has used the crime/fraud exception to the attorney-client privilege to pierce the privilege and discover attorney files regarding the implementation and administration of a records and information management program. *See Rambus, Inc. v. Infineon Techs. AG*, 220 F.R.D. 264, 281 (E.D. Va. 2004). Other sanctions may include the award of attorney's fees and expenses for the non-spoiling party, the exclusion of testimony or evidence on the subject or defense to the document allegedly destroyed, or ordering the spoiling party to pay for the restoration of the remaining backup tapes and the re-taking of depositions based on such retrieved information. *Zubulake V*, 229 F.R.D. at 437-440.

Of course, the "ultimate sanction" to be imposed by a court is the entry of a default judgment against the party found to have intentionally altered or destroyed evidence. *See Carlucci*, 102 F.R.D. at 480-486. For example, in *Wm. T. Thompson Co. v. Gen. Nutrition Corp., Inc.*, 593 F. Supp. 1443 (C.D. Cal. 1984), the District Court for the Central District of California entered a default judgment against the defendant because the defendant failed to preserve relevant documents after it received document requests and the court ordered document preservation. *Wm. T. Thompson Co.*, 593 F. Supp. at 1456 ("Default and dismissal are proper sanctions in view of [defendant's] willful destruction of documents and records that deprived [plaintiff] of the opportunity to present critical evidence on its key claims to the jury"). The District Court for the District of Connecticut entered the same sanction where defendants willfully violated discovery orders by failing to turn over general ledgers, lying about their inability to obtain documents, and destroying documents. *See S. New Eng. Tel. Co. v. Global NAPs, Inc.*, C.A. No. 3:04-cv-2075, slip op. (Conn., June 23, 2008)[available at 2008 U.S. Dist. LEXIS 47986]. However, courts are unlikely to enter a default judgment or dismiss a

case unless no other sanction will remedy the spoliation. See Kindel & Richter, *supra.*, 27 Wm. Mitchell L. Rev. at 687.

D. What Effect Does A Records and Information Management Program Have On The Duty To Preserve?

The United States Supreme Court has acknowledged that “[d]ocument retention policies, which are created in part to keep certain information from getting into the hands of others, including the Government, are common in business.” *Arthur Andersen LLP v. United States*, 544 U.S. 696, 704 (2005)(citing Chase, *To Shred or Not to Shred: Document Retention Policies and Federal Obstruction of Justice Statutes*, 8 Ford. J. Corp. & Fin. L. 721 (2003)). More importantly, the United States Supreme Court has stated that “[i]t is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances.” *Arthur Andersen LLP*, 544 U.S. at 704. In light of these acknowledgements, the question arises as to what effect does a document retention and litigation hold policy have on the duty to preserve.

As evidenced in *Lewy*, where the Eighth Circuit stated in dicta that a company’s document retention policy does not automatically protect it from spoliation claims, courts have begun to address whether the existence and a company’s compliance with a document retention policy will shelter the company from spoliation claims. For example, courts have ruled that document retention policies that were established in bad faith, such as shortly before a known claim was filed, will not shelter a company from spoliation claims. See, e.g., *Capellupo v. FMC Corp.*, 126 F.R.D. 545 (D. Minn. 1989). Likewise, if a document retention policy’s design allows for the destruction of documents before the statute of limitations has run on a claim that could involve the destroyed evidence, see, e.g., *Reingold v. Wet N’ Wild Nevada, Inc.*, 944 P.2d

800 (Nev. 1997), or if a company fails to ensure that its employees preserve relevant evidence, see, e.g., *Metropolitan Opera Assoc. v. Local 100, Hotel Employees and Rest. Employees Int’l Union*, 212 F.R.D. 178 (S.D.N.Y. 2003), then the courts are unlikely to hold that the existence of a document retention and litigation hold policy will protect the company from a spoliation claim.

Nevertheless, “[c]ourts routinely refuse to invoke sanctions against corporations that dispose of documents without bad faith and pursuant to a legitimate and uniformly applied record retention policy, sometimes even in the face of pending litigation.” Kinsler & Keyes MacIver, *supra.*, 34 Tort & Ins. L.J. at 772-73. For instance, courts have held that even when litigation was pending, sanctions for spoliation were inappropriate where the subject records were destroyed pursuant to a document retention policy by an employee who was not aware the records were to be preserved. See, e.g., *Coates v. EEOC*, 756 F.2d 524 (7th Cir.1985); *Wright v. Illinois Cent. R.R. Co.*, 868 F. Supp. 183 (S.D. Miss. 1994).

Consequently, what should you and your company do to ensure that its record and information management program will shelter it from spoliation claims? Initially, you and your company should consider the following when establishing and implementing the policy:

- * When, how and why does the policy appear to be established?
- * Is the policy designed to ensure that no documents are destroyed prior to the applicable statute or regulation or, where applicable, the statute of limitations?
- * Is the policy regularly implemented, so that documents are destroyed pursuant to the schedule and not just before litigation is threatened?
- * Have the terms of the retention policy been communicated to all relevant employees, such that the employees are advised when litigation is pending or threatened and that the policy should be suspended?

Further, in establishing and implementing a records and information management program, companies should avoid certain activities, such as:

- * Establishing a document retention strategy for the principal apparent purpose of preventing the use of business records in subsequent litigation;
- * Failing to make reasonable efforts to communicate the fact of pending or future litigation to employees responsible for purging files or implementing routine document disposal;
- * Automatically applying the policy despite circumstances calling for a responsive suspension or revision;
- * Engaging in unusual or sporadic destruction of documents, *i.e.*, failing unreasonably to adhere to the policy in a coherent manner.

Kinsler & Keyes MacIver, *supra.*, 34 Tort & Ins. L.J. at 783.

Furthermore, to ensure your company's good faith in establishing and implementing a records and information management program, the company should outline, in memorandum form, the reasons for establishing and implementing program and maintain a document retention schedule that catalogs the company's documents, the laws and regulations that govern the retention of those documents and the length of time such documents need to be preserved. An example of such an outline and retention schedule is provided in Appendix.

Notification of your company's records and information management program and the need to preserve documents when a litigation hold is imposed is the most integral part of an effective and compliant program. In other words, the existence of records and information management program will not be, in and of itself, sufficient to avoid sanctions if the program's policy and procedures are not properly implemented or disseminated to employees, or, in the case of litigation, the notification sent to employees regarding their duty to preserve fails to advise the key employees of the need to preserve all relevant evidence.

An example of the importance of notification can be found in the case of *Wiginton v. CB Richard Ellis*, No. 02 C 6832, slip op. (N.D. Ill. Oct. 27, 2003)[available at 2003 U.S. Dist. LEXIS 19128], *motion granted in part and denied in part* 229 F.R.D. 568 (N.D. Ill., Aug. 9, 2004). In *Wiginton*, the magistrate judge held that CB Richard Ellis' notification to its employees to preserve documents was too narrow in scope because it only advised employees to retain documents that applied to the plaintiff and did not advise employees to retain other documents that might be relevant to the class action litigation filed by the plaintiff. *Wiginton*, 2003 U.S. Dist. LEXIS 19128, at *14-*17. In other words, the notification to CB Richard Ellis' employees was inadequate because it "never informed its employees about the need to retain any documents that might be relevant to the lawsuit, as opposed to any documents dealing specifically with [the plaintiff]." *Id.* at *14-*16. Additionally, the magistrate judge found that CB Richard Ellis violated its duty to preserve because the company maintained its "normal document retention and destruction policies [and] did not inform its director of network services that any electronic information should be retained" *Id.* at *23-*25. Thus, the magistrate judge held that CB Richard Ellis acted in bad faith by failing to change its normal document retention policy, but denied the plaintiff's motion for sanctions. *Id.* On appeal, the district court affirmed the magistrate judge's finding, but awarded the plaintiff only 25% of the costs incurred to recover relevant documents from backup tapes. *Wiginton*, 229 F.R.D. at 577.

Another example of the importance that a company provide notification of its records and information management program and the need to preserve documents when a litigation hold is imposed is *In re Prudential Insurance Co. of America Sales Practices Litigation*, 169 F.R.D. 598 (D.N.J. 1997). The *Prudential Insurance* case involved a class action brought by Prudential policyholders who accused Prudential Insurance of engaging in deceptive sales practices when

selling life insurance. *Prudential Ins.*, 169 F.R.D. at 600. In response to the court's preservation order, which required Prudential Insurance to "preserve all documents and other records containing information potentially relevant to the subject matter of [the] litigation," Prudential Insurance sent out several e-mails informing its employees of the need to preserve documents. *Id.* at 612. However, as the district court noted, the e-mails were typed in ordinary font and ignored by several employees, not all employees had access to the e-mail system, and the e-mails were not printed or otherwise made available to those employees who did not have access to e-mail system. *Id.* at 613. The district court recognized that there was "no proof that Prudential, through its employees, engaged in conduct intended to thwart discovery through the purposeful destruction of documents." *Id.* Nevertheless, the district court found that Prudential Insurance's "haphazard and uncoordinated approach to document retention indisputably denies its party's opponents potential evidence to establish facts in dispute." *Id.* Further, the district court held that after it ordered Prudential Insurance to preserve documents, "it became the obligation of senior management to initiate a comprehensive document preservation plan and distribute it to all employees." *Id.* "Moreover, it was incumbent on senior management to advise its employees of the pending multi-district litigation . . . , to provide them a copy of the Court's Order, and to acquaint its employees with the potential sanctions, both civil and criminal, that the Court could issue for noncompliance" with the order. *Id.* Because none of these acts were taken, the district court imposed a **one million dollar sanction** on Prudential for its senior management's failure to adequately notify and disseminate information regarding the need to preserve documents, stating that the "obligation to preserve documents that are potentially discoverable materials is an affirmative one that rests squarely on the shoulders of senior corporate officers." *Id.* at 615. *See also Danis v. USN Communications, Inc.*, 53 Fed. R. Serv. 3d

(Callaghan) 828 (N.D. Ill. Oct. 23, 2000)[available at 2000 U.S. Dist. LEXIS 16900](although the district court refused plaintiff's request for the entry of default judgment, the court imposed a \$10,000 fine upon the defendant's chief executive officer who "personally took no affirmative steps to ensure" documents were not destroyed and "attempted to delegate that responsibility completely" to in-house counsel who did not have any litigation experience and who did "nothing to ensure that all USN employees who handled documents that might be discoverable were aware of the lawsuit and the need to preserve documents ...").

III. USE OF THIRD-PARTY EXPERTS

Not every claim or dispute in which your company will become involved will require the services of e-discovery or computer forensics specialist. In fact, certain cases or matters can be handled efficiently and effectively without ever having to address any issues as to ESI. However, in today's business world, it is quite common that some portion of a claim or dispute will involve records or information that is electronic in nature. Thus, if a claim or dispute involves ESI, then your company will probably need the help of either an e-discovery or a computer forensics expert.

For many, the customary case does not warrant the excessive fees that can mount from engaging an e-discovery or computer forensics expert. Instead, your company may be best served by engaging an e-discovery or computer forensic expert to retrieve the pertinent evidence for you and your outside counsel and then having your outside counsel do his or her own review, making certain not to destroy, damage or otherwise spoil the evidence by such review. In this situation, the charges for an e-discovery or computer forensics specialist will likely be \$5,000-to-\$10,000.

On the other hand, if you are involved in a multi-million dollar case involving terabytes of data, then your company will probably need to engage a company that can handle not only the management of e-discovery, but also all of the computer forensics needs. Generally, such a company will have data-hosting capacity and if they do not, they undoubtedly will be able to refer you to a company that offers such service. Under this scenario, the cost for the ESI services will likely be thousands if not hundreds of thousands of dollars.

In the end, selecting the appropriate experts to work with is the most important decision that you, as general counsel, may make when your company becomes involved in a matter involving ESI. One of the most common mistakes that companies and their lawyers make when handling a case involving ESI is selecting the wrong experts. However, with thought and care, you can avoid the mistakes that are commonly made and handle cases involving ESI with the assistance of the proper expert.

The following are some guidelines that you and your company should consider in determining what type of ESI expert should be hired and how you and your company should work with such expert:

- **The Type of Expert Needed.** Many computer forensic technologists can perform e-discovery tasks. However, few e-discovery experts can perform actual computer forensics. In short, computer forensics means performing a forensic acquisition of a hard drive or other media and extracting and documenting the data. In contrast, e-discovery generally concerns the analysis and manipulation of the data once it has been extracted. The two tasks are not the same and should not be confused.

- **Forensics Certifications.** Currently, the EnCase Certified Examiner (“EnCE”) issued by Guidance Software is the most prestigious certification available to private firms engaged in computer forensics. Another well-known certification is the Certified Information Forensics Investigator (“CIFI”) issued by the International Information Systems Forensics Association (“IISFA”), a nonprofit organization. As time progresses, more certifications will emerge and gain credibility. However, in the private sector, the EnCE and the CIFI are the most prominent certifications. **NOTE:** Many “experts” will claim certifications or degrees on their CV when the truth is that they merely took classes or attended training courses. In such situations, no real meaningful certification is granted; instead, just a “certification of attendance” has been received. If you see a certification on a person’s resume that you don’t recognize, then you need to ask questions. For example, was a written examination or test was required? Was the applicant required to spend and document a minimum amount of time that he or she had been involved in computer forensics? Was the expert certified in computer forensics or merely in the use of a particular forensics tool or program? What are the credentials of the organization that issued the certification? Who was on the organization’s faculty? Is there a recertification component and if so, what are the parameters of the recertification? If you fail to ask these questions, the computer forensics “expert” that you have engaged may not be worth much as an expert.
- **Technical Certifications.** A good forensic technologist will have a lot of letters after his or her name, indicating a broad range of certifications with a number of

different technologies. If you see no certifications, or a “base-level” certification (such as A+), you do not have an individual with a wealth of experience. For example, if the expert is a Certified Novell Engineer, Certified Cisco Network Administrator, Microsoft Certified Professional + Internet, Microsoft Certified Systems Engineer, NT Certified Independent Professional, and a Certified Internetwork Professional, then this person is someone with an expansive technical background.

- **The CV.** Get the expert’s CV early on and study it. Don’t be afraid to ask questions. Does it show that the expert has spoken at a lot of seminars and/or written a lot of articles? Those who present or teach frequently and have to answer questions on the fly tend to be excellent testifying experts. Also, teaching and authorship frequently add credibility with a judge or jury. What is the expert’s educational and professional background? Is this a broad-based technologist or someone who is a new college grad and wet behind the ears or with just a sliver of technical knowledge? Beware of the individual who claims multiple disciplines. Whether a private detective, computer repairman, or software engineer, or some combination of many things, a forensic technologist worth having is generally billed as a forensic technologist and does not offer a Chinese buffet of services.
- **Court Qualifications.** Good experts have qualified in multiple courts, and those courts and cases should be all listed on the CV. Granted, most cases of any kind tend to settle; so, even the best of experts may have limited court appearances. Nevertheless, you should be wary of someone who has limited or no court qualifications.

- **Chain of Custody.** In today’s world, it is not necessary that your computer forensics’ expert be in the same location as you. You can maintain chain of custody perfectly well by shipping a computer from Pittsburgh to Chicago if that’s where the best expert is located. Although local experts may be preferred in cases where paying for travel expenses may be an issue, you should not let an expert’s location serve as a reason for not employing the best possible computer forensic technologist. If the case has a significant amount at stake and/or may well end up in trial, you do yourself a disservice by restricting your selection to local experts.
- **Confidentiality.** Not all cases are shrouded in secrecy, but a fair proportion of them are. Make sure the expert you pick has a confidentiality clause in the retainer agreement, and don’t hesitate to ask the expert to sign your own confidentiality agreement. Remember as well that the expert may be working on your case with others and that the entire firm should have an impeccable reputation for keeping your company’s secrets. During the course of a major case where the expert has been identified, the press will undoubtedly come sniffing around the expert probing for information. A good expert knows the standard answer, “I’m sorry, I have no comment.”
- **Communication.** An expert must speak the English language clearly and with as little reference to technical jargon. If an expert is unable to speak clearly and communicate in lay terms, with analogies that a judge or jury can understand, then he is not an expert witness that you’ll want to have.

- **Fees and Costs.** E-discovery and computer forensics are not cheap. Small cases may run in the \$5,000–\$10,000 range, but larger cases can hit six figures with astonishing rapidity. It is almost never possible to quote a probable final figure at the outset of the case, because the third-party expert has not yet seen the “size of the elephant.” It will generally require some time into the case before it is possible to let a client know how much work will ultimately be involved. It is often the same predicament that lawyers face when trying to give clients a rational estimate. As a general rule, the larger the forensics firm, the larger the bill. It is not uncommon to pay as much as \$500/hour in the largest firms. In high-quality but smaller firms, \$250–\$350/hour may be a more common charge. If the third-party expert charges less than \$200/hour, you should seriously investigate the firm credentials, references, number of courts qualified in and standing in the industry. **NOTE:** Some technologists bill fairly. They turn their clocks off while a process is running and go work on someone else’s case. They account for their time accurately and precisely. On the other hand, there are those (often with lower rates), who charge you for every moment they are at work—and sometimes beyond. In the end, getting references is your best bet here.
- **References.** One of the best ways to find a good computer forensics technologist is to ask your potential expert for references and then speak with those references. Some of the questions that you should ask the references of a potential expert are the following: What type of work or tasks did the expert perform? Was the expert’s work thorough and professional? Did the expert respond in a timely manner? What was the quality of the expert’s report? Did the expert make a

credible witness? Did the expert give you honest, truthful answers or was he or she more interested in telling you what you wanted to hear? Did the expert stay within budget or, if not, alert you to additional costs before incurring them?

- **Investigate Your Expert.** In addition to checking up with your potential expert’s references, you should also investigate the expert to verify his or her credentials. As set forth more fully in Section V.E below, there are many on-line tools that you can use to find and locate information on potential expert witnesses, including computer forensic technologists. In fact, a search using Google and other Internet search engines may reveal articles and presentations authored by your potential expert, as well as whether your expert has ever been disciplined or decertified.
- **Evidence Format.** What format do you want/need the evidence in? Is it to be placed on CDs, DVDs or a hard drive? Can you read the evidence in its native format or do you need it converted? Should it be ready for importing into Concordance or Summation? Is your expert familiar with and licensed to use the format selected?
- **The Expert’s Contract.** It is important for you to read and understand the terms of the contracts for third-party experts. You must make sure the contract contains a confidentiality provision and that the billing terms and fees are clearly spelled out. If there are “caps” or “do not exceed without written authorization” provisions, make sure they are adequately expressed. You need to know what your expert must do if they run into child pornography or other potentially criminal material. Who is to sign the contract? Frequently, especially in the cases

of a non-testifying expert, your lawyer will wish to sign the contract in order to invoke the work-product doctrine where applicable.

- **Scope of Engagement.** It is important that you ascertain and define the scope of work each expert can and will accomplish. The lines between computer forensics and e-discovery are blurred, so it is helpful to inquire whether the computer forensics or e-discovery expert is qualified to help draft pleadings, provide the technical questions at depositions, or has legal counsel on staff to ascertain the legal relevance of unearthed data.
- **Preservation of Electronically Stored Data.** Do not go stomping all over the evidence yourself (or let your IT department do that). When computer forensics specialists get together and swap war stories, one recurrent theme is the unbelievable number of times that clients have fouled themselves up by trampling ESI. Typically, as soon as a potential legal matter is recognized, a law firm or corporation authorizes someone from its IT department to “look through” the evidence. Unbeknownst to them, while their IT staff is busy finding golden nuggets of evidence, they are also changing the dates and times of the files they are accessing and possibly altering information that indicates which user ID did what. Although it may not entirely discredit the case, you have now given fodder to opposing counsel at the very least—and you will have to spend more money on the forensic examination because unraveling dates and times and explaining “the stomping” effect is now part of the examiner’s job. It is a very foolish client that contaminates evidence by having in-house folks look at it—from a judge’s or

jury’s point of view, the client has a vested interest in that evidence. Far more credible is an initial, independent forensic examination by a certified third party.

- **Educate the Expert.** Just like any other expert, an e-discovery expert should be provided with copies of the original pleadings, or (prelitigation) a statement of case facts. It is astonishing how often lawyers will leave their experts with only a minimal understanding of case facts and simply give them a set of instructions. Experts worth their salt will carefully review any pleadings or case facts so they know what they are looking for. Often, lawyers and clients produce keywords that make no sense or they give their experts wonderfully vague instructions, such as “poke around and see what you can find.” Even a little knowledge goes a long way toward helping an expert do a good job, thereby reducing the time and cost of analysis.
- **Litigation Support.** Good lawyers are smart enough to know what they do not know. If you are not a technologist, how are you going to draft proper complaints, motions, discovery pleadings, and so forth that relate specifically to technology? It may well be that your expert is only needed to help you with slices of the documents, but it behooves the lawyer to make full use of the expert to make sure those slices are appropriately drafted. If you don’t understand technology, your attempt to depose an IT administrator is likely to be a disaster. You may have the list of questions prepared by your expert, but in all likelihood, you’ll ask some preliminary question about system authentications, and the answer you receive will sound to you like “Blah blah blah blah blah.” Only if your expert is present or asking the questions can appropriate follow-up questions

be addressed. In addition, your expert can screen for the nonsense factor, which is likely to completely elude someone without a technical background. Experts can be an enormous help in trial preparation and can often see the technical questions that may be raised on the other side and help construct answers.

- **Avoid Misunderstandings.** If you want your computer forensics technologist to simply acquire evidence and then turn that evidence over to you or your lawyer or to an e-discovery firm, let the technologist know that. If either one is supposed to convert evidence to a particular format and then turn the evidence over to you or your lawyer for analysis, make sure they know. If you want a preliminary report after a few hours of work, to ascertain “the size of the elephant” and the costs, make sure your expert knows that. If money is an issue, and you’d like your expert to tell you when charges reach a specified sum, make that clear—in writing.
- **Written Reports.** You should discuss with your third-party witnesses what exactly you would like in writing and when. Bear in mind that there will always be, depending on the particular computer forensics/analysis software used, some sort of report and documentation. This report, however, will constitute a simple explanation of what was done and what was found—expert opinions are another creature entirely. Remember that even drafts of expert opinions have been found to be discoverable. This is problematic, because there are many sound reasons why drafts will change—nonetheless, the alterations may provide fodder for the other side.

- **Look for The Truth, Not The Smoking Gun.** There is nothing more gratifying than finding a digital smoking gun (especially, when the subject of the e-mail message is titled “Smoking Gun”). However, sometimes after hours or days of searching and analyzing, it becomes painfully evident that what the client hoped to find is simply not there. At times, lawyers or their clients become agitated and even fixated on the notion that what they are looking for must be there. If you have a competent, certified forensic examiner, or e-discovery expert, believe her if she says she has followed all appropriate procedures and the evidence you are looking for is not there. Perhaps the evidence never existed at all, or it may have been overwritten (and therefore unrecoverable), or the drive/specific files may have been wiped, sometimes with a special utility, or it resides on a different computer or system. Under no circumstance should you ask your expert to bear false witness.
- **Be Fiscally Prudent, But Not Cheap.** Forensic acquisition and data analysis are slow, painstaking functions that, done correctly, are part of a scientific process punctuated by constant documentation of work done. Nonetheless, lawyers (and clients) frequently seem to think that “Filene’s Basement” prices should apply. It is wise to get your expert’s “best guess” up front and then to reevaluate after the expert has had a chance to immerse him or herself in the case facts and the data. Keeping the client in the loop is always helpful. It should be possible for client, lawyer, and expert, working together, to come up with a rational set of numbers before the case has progressed too far. Remember that on-site work is always more expensive than work experts can do in their labs. A lab has the fastest

equipment and the expert is surrounded by the entire forensic toolkit at his or her command.

APPENDIX

<u>Form No.</u>	<u>Description</u>
I.A	Preliminary Questions for IT Department
I.B	Checklist to Define Scope of Electronically Stored Information
I.C	Checklist to Define Sources of Electronically Stored Information
II.A	Sample Document Retention Policy for Small Business
II.B	Sample Records Management Policy Statement (ARMA)
II.C	Sample Records Retention and Destruction Policy
III	Sample Record/Information Retention Schedule
IV.A(1)	Sample Preservation Notice to Employees/Agents
IV.A(2)	Sample Preservation Notice to Employees/Agents
IV.B	Sample Preservation Notice to Adverse or Third Parties
IV.C	Sample Preservation Notice to Opposing Counsel
V	Investigating Expert Witnesses via the Internet

Form I.A**Preliminary Questions for IT Department**

1. Provide detailed description of computer systems used by the company, including hardware systems, primary operating systems, and major software systems, including any customized software.
2. Provide a detailed description of how those computers are networked or connected to others outside of the company (with a graphical representation if one is available).
3. Provide a detailed description of how your employees can network with your computers from outside of the company.
4. Provide a detailed description of the computer systems used by your employees outside of the corporate system (e.g., from home desktops or laptops, personal digital assistants [PDAs]).
5. Provide a detailed description of the backup processes and schedules, document 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.
6. Provide the company's document retention policy, e-mail, and Internet-usage policies and litigation-hold policy, to the extent they exist.
7. Describe any monitoring or logging of employees' computer usage.
8. If any third parties hold or have access to the company's data, identify those third parties with full contact information.

Form I.B**Checklist to Define Scope of Electronically Stored Information**

To facilitate the retention, destruction and preservation (if warranted) of electronically stored information, the following elements should be identified:

1. 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.
2. 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.
3. The architecture of the electronic mail system, including, but not limited to, server and workstation software and version, lists of users, and location of e-mail files.
4. Enterprise user information applications, including, but not limited to, contact lists, calendars, to-do lists, word processing, project management, and accounting.
5. Internal and external personnel responsible for the management and maintenance of the technology infrastructure and all of its components, with contact information.
6. Information about any business activity of employees that is not backed up by the company, including the use of home machines, laptops, PDAs, etc.
7. The names of all key players in any actual or potential lawsuit or investigation.
8. The names, addresses, and contact info for any third party that holds or has access to company data.
9. 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.
10. 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.
11. The location and contents of any relevant system and event logs.

Form I.C**Checklist to Define Sources of Electronically Stored Information**

The following is a sample list of common sources for electronically stored information:

Electronic Information

1. Servers, including virtual servers
2. Mainframes
3. Network file systems
4. Workstations or desktop computers
5. Laptop or notebook computers
6. Personal digital assistants (PDAs)
7. Personal home computers
8. Private branch exchange (PBX)
9. Voice mail
10. Digital printers or copiers
11. Cell phones, Smartphones & BlackBerry devices

Backup Media

12. Monthly system wide backups
13. Weekly system wide backups
14. Incremental system wide backups
15. Unscheduled backups
16. Personal backups

Additional Media Devices

17. CD-ROMs
18. DVDs
19. Floppy diskettes
20. Zip disks
21. Tape archives
22. Removable hard drives
23. Thumb drives (such as Flash Memory, USB Memory Stick, Jump Drive, etc.)
24. Digital camera media

Form II.A**Sample Document Retention Policy for Small Businesses**

NOTE: This form policy is intended for small businesses that are not subject to specific regulatory requirements.

DOCUMENT RETENTION POLICY

The corporate records of COMPANY, and its subsidiaries (hereafter the "Company") are important assets. Corporate records include essentially all records you produce as an employee, whether paper or electronic. A record may be as obvious as a memorandum, an e-mail, a contract, or a case study or something not as obvious, such as a computerized desk calendar, an appointment book, or an expense record.

The law requires the Company to maintain certain types of corporate records, usually for a specified period of time. Failure to retain those records for those minimum periods could subject you and the Company to penalties and fines, cause the loss of rights, obstruct justice, spoil potential evidence in a lawsuit, place the Company in contempt of court, or seriously disadvantage the Company in litigation.

The Company expects all employees to fully comply with any published records-retention or -destruction policies and schedules, provided that all employees should note the following general exception to any stated destruction schedule: If you believe, or the Company informs you, that Company records are relevant to litigation, or potential litigation (i.e., a dispute that could result in litigation), you must preserve those records until the Legal Department determines the records are no longer needed. That exception supersedes any previously or subsequently established destruction schedule for those records. If you believe that exception may apply, or have any question regarding the possible applicability of that exception, please contact the Legal Department.

From time to time the Company establishes retention or destruction policies or schedules for specific categories of records in order to ensure legal compliance and also to accomplish other objectives, such as preserving intellectual property and cost management. Several categories of documents that bear special consideration are identified below. Although minimum retention periods are suggested, the retention of the documents identified below and of documents not included in the identified categories should be determined primarily by the application of the general guidelines affecting document retention identified above, as well as any other pertinent factors.

1. **Tax Records.** Tax records include, but may not be limited to, documents concerning payroll, expenses, proof of deductions, business costs, accounting procedures, and other documents concerning the Company's

revenues. Tax records should be retained for at least six years from the date of filing the applicable return.

2. **Employment Records/Personnel Records.** State and federal statutes require the Company to keep certain recruitment, employment, and personnel information. The Company should also keep personnel files that reflect performance reviews and any complaints brought against the Company or individual employees under applicable state and federal statutes. The Company should also keep all final memoranda and correspondence reflecting performance reviews and actions taken by or against personnel in the employee's personnel file. Employment and personnel records should be retained for six years.
3. **Board and Board Committee Materials.** Meeting minutes should be retained in perpetuity in the Company's minute book. A clean copy of all Board and Board Committee materials should be kept for no less than three years by the Company.
4. **Press Releases/Public Filings.** The Company should retain permanent copies of all press releases and publicly filed documents under the theory that the Company should have its own copy to test the accuracy of any document a member of the public can theoretically produce against the Company.
5. **Legal Files.** Legal counsel should be consulted to determine the retention period of particular documents, but legal documents should generally be maintained for a period of ten years.
6. **Marketing and Sales Documents.** The Company should keep final copies of marketing and sales documents for the same period of time it keeps other corporate files, generally three years.

An exception to the three-year policy may be sales invoices, contracts, leases, licenses, and other legal documentation. These documents should be kept for at least three years beyond the life of the agreement.
7. **Development/Intellectual Property and Trade Secrets.** Development documents are often subject to intellectual property protection in their final form (e.g., patents and copyrights). The documents detailing the development process are often also of value to the Company and are protected as a trade secret where the Company:
 - (a) derives independent economic value from the secrecy of the information; and
 - (b) the Company has taken affirmative steps to keep the information confidential.

The Company should keep all documents designated as containing trade secret information for at least the life of the trade secret.
8. **Contracts.** Finally, execution copies of all contracts entered into by the Company should be retained. The Company should retain copies of the

final contracts for at least three years beyond the life of the agreement, and longer in the case of publicly filed contracts.

9. **Electronic Mail.** E-mail that needs to be saved should be either:
 - (a) printed in hard copy and kept in the appropriate file; or
 - (b) downloaded to a computer file and kept electronically or on disk as a separate file.

The retention period depends upon the subject matter of the e-mail, as covered elsewhere in this policy.

Failure to comply with this Document Retention Policy may result in punitive action against the employee, including suspension or termination. Questions about this policy should be referred to [name] ([phone]; [e-mail address]), who is in charge of administering, enforcing, and updating this policy.

READ, UNDERSTOOD, AND AGREED:

Employee's Signature: _____ Date: _____

Form II.B
Sample Records Management Policy Statement
(As published by the American Records Management Association)

Policy Purpose: To provide guidelines for properly establishing a records and information management (RIM) program and assisting those departments that require long-term records retention and procedures for implementing an effective RIM program. Records and information management includes areas such as inactive records, vital records, microfilming, and records retention.

Policy

1. Records and information management (RIM) is the systematic control of all records, regardless of media, from their creation or receipt, through their processing, distribution, organization, storage, and retrieval to their disposition. Information flows through the organization in the form of paper and electronic records such as word processing documents, spreadsheets, e-mail, graphical images, and voice or data transmissions. Information can be stored on a variety of storage media, such as microfilm, microfiche, diskette, optical disk, CD-ROM, videotape, and paper.
2. This policy details the requirements and responsibilities to initiate a well-defined RIM program. The RIM program applies to those departments that require a long-term records-retention, -storage, and -destruction program.
 - a. Ensure only essential records of continuing value are preserved. Records should be retained in the active office areas as long as they serve the immediate administrative, legal, or fiscal purpose for which they were created.
 - b. Establish safeguards against the illegal removal, loss, or destruction of records. Records either should be disposed of in accordance with an approved records-retention schedule or transferred to the records-retention center until the prescribed retention period has expired.
 - c. Management of records is the responsibility of the owner, or creator, of the record. The department director or the director's designated representative should contact the records manager to discuss initiating a records-management program or reviewing an existing records-management program to handle records properly from their creation through their destruction. Departments can be provided guidance on how records should be organized and stored to ensure timely and efficient retrieval.
 - d. The records-retention schedule is the key tool for departments to use to manage their records effectively. Information is a valuable asset; however, if records that contain information cannot be retrieved efficiently or are retained beyond their legal, regulatory, or administrative retention period, they lose their value and may impose a liability to the organization.
3. The benefits of an effective RIM program include:
 - a. Greater assurance of legal compliance to minimize liability and discovery impacts;
 - b. Improved customer service with higher quality of service and faster retrieval of documents;
 - c. Improved staff productivity with effective records-management systems;
 - d. Reduced storage costs through elimination of unnecessary and duplicate documents;
 - e. Ensured safety of vital organizational records; and
 - f. Efficient, cost-effective records-retention and -disposal system.
4. The components of an effective RIM program that may be activated by the records manager include:
 - a. Records-retention program;
 - b. Vital records program;
 - c. Inactive records-management program;
 - d. Electronic records-management program;
 - e. Records-management handbook/records liaisons' training;
 - f. Micrographics (microfilming) program;
 - g. Forms-management program (corporate communications);
 - h. Active records-management program; and
 - i. Copy and reprography program (purchasing).
5. Significant recurring activities initiated by the records manager include:
 - a. Annual inventory of the records center: The records manager will annually inventory all records in the records center to confirm information in the records-retention tracking system.
 - b. Annual review of the records-retention schedule: The records manager will have the records-retention schedule reviewed and validated annually for accuracy.
 - c. Annual files purge program: The records manager will advertise and initiate an annual files purge by all departments. The purpose is to have individuals review personal active file systems, as well as electronic document folders, and to purge documents that are no longer required. No original documents are to be destroyed.

Proponent

1. The vice president for information systems or his designee is the proponent for the RIM program.
2. All questions concerning compliance with this policy should be directed to the records manager unless otherwise indicated.

Roles and Responsibilities

1. The vice president of finance, vice president of legal affairs, and the chief information officer, as needed, will be requested to identify to the records manager the individual who can perform the following tasks:
 - a. Review and provide functional approval of an updated or changed records-retention schedule, as required, for all departments.
 - b. Become familiar with the purpose of the records-retention schedule.
2. Department directors who need to implement a records-management program should contact the records manager for guidance/assistance and will need to:
 - a. Identify a records liaison and inform them of the duties of the records liaison;
 - b. Review and update records-retention schedules annually;
 - c. Review the records-management handbook, as needed; and
 - d. Coordinate departmental activities that may impact records management with the records manager to include office consolidation, office closures, and approval of new or replacement, records storage, and file equipment as requested.
3. Departmental records liaisons are responsible for:
 - a. Obtaining records liaisons' overview training from the records manager;
 - b. Becoming familiar with and maintaining the records-management handbook;
 - c. Assisting in developing and enforcing the records-retention schedule for their department;
 - d. Managing the department's records; and
 - e. Attending quarterly or as otherwise required records liaisons' meetings.
4. Records manager is responsible for:
 - a. Assisting in the design, development, implementation, and/or review of records-management programs to include the programs listed in paragraph 2, Policy, above;

-3-

© Copyright 2008. Ronald L. Hicks, Jr. All Rights Reserved.

- b. Managing the records-retention center for all departments to ensure safe storage, quick retrieval, records confidentiality, and appropriate records disposition;
- c. Developing and maintaining the records-retention schedule;
- d. Managing the microfilming of records as required;
- e. Issuing and updating the records-management handbook;
- f. Educating and training records liaisons;
- g. Approving records storage and retrieval equipment for departmental purchase as requested;
- h. Participating actively as a member of the following committees:
 - i. Records Committee on an as-needed basis for retention issues;
 - ii. Forms Approval Committee as a member on an as-needed basis;
- i. Presenting records and information management issues, as required, to the Information Systems Steering Committee or other appropriate forum; and
- j. Chairing quarterly Records Management Committee meeting with records liaison.

Procedures

Detailed procedures can be found in the records-management handbook. For the most frequent requirements, procedures are summarized below.

1. Records-Retention Schedules
 - a. Each department is responsible for determining retention periods for records created. A record may be kept beyond the legal or regulatory retention period if it satisfies an administrative need based on business necessity, which is stated on the records-retention schedule. To create or update a records retention schedule:
 - i. Contact the records manager to assist you;
 - ii. Inventory all current records maintained, including all media types;
 - iii. Create a master list of data and record types and draft preliminary retention schedule;
 - iv. Determine retention periods based on legal, administrative, and historical value;
 - v. Obtain approval for retention schedule from IS, Finance, and Legal;

-4-

© Copyright 2008. Ronald L. Hicks, Jr. All Rights Reserved.

- vi. Publish and implement the retention schedule; and
 - vii. Review annually.
 - b. State, federal, and/or regulatory requirements prescribe minimum records-retention periods.
 - c. Once the specific retention period for any paper or electronic record has been reached, the record will be destroyed consistent with appropriate procedures.
 - d. Notwithstanding minimum retention periods, all records shall be maintained until all required audits are completed and shall be kept beyond the listed retention period if litigation is pending or in progress. Records manager must be notified of any litigation that would require retention of records beyond normal disposition.
 - e. Destruction of records is permitted in accordance with the law only after expiration of the retention periods stated on the approved departmental retention schedules.
2. Files Transferred to Records Center
- a. Files will be accepted throughout the year once the department has coordinated set patterns for retention with the records manager.
 - b. The departmental records liaison will contact records manager via e-mail of a files transfer requirement.
 - c. Storage boxes and Records Center Control Card Form must be obtained from records management.
 - d. Files must be packed in approved storage boxes.
 - e. A Records Center Control Card Form must accompany the boxes.
 - f. Records management will provide instructions for proper packing and labeling of boxes in the records-management handbook.
 - g. Pickup will be coordinated with records manager.
3. Request for Retrieving Files or Records
- a. Office wishing to retrieve records will contact the records-retention center.
 - b. The departmental records liaison will provide information for locating the file from the Records Center Control Card.
 - c. Telephone request should not exceed five (5) records per call. For more than five records, a written request should be mailed or e-mailed to records management.
 - d. Retrieved records will be tagged with a Records Center Reference Request form. This form *must* be returned to allow prompt and accurate re-filing.

-5-

© Copyright 2008. Ronald L. Hicks, Jr. All Rights Reserved.

- e. Notify records management if file is to be reactivated.
4. Microfilming Records
- a. Medical records will be microfilmed in records management and stored in the information services department for reference and retrieval.
 - b. Other departmental records meeting certain specifications will be microfilmed and stored within the department or in records management. This should be coordinated with the records manager.
5. Assistance in the Selection of Records Filing System Equipment
- a. All new records-management and filing equipment should be reviewed by the records manager, as requested, prior to purchase to ensure they are efficient and cost-effective in storage space.
 - b. Existing file systems can be reviewed and recommendations provided for improvement.
6. Records-Retention Requirements for Automated Systems
- a. Systems and programming managers will contact the records manager who will assist the department that owns the data in determining records-retention requirements for the electronic data on new and existing systems.
 - b. A valid retention schedule will be prepared for electronic records.
7. Vital Records Program

The implementation of a vital records program to protect and preserve records that contain information vital to the conduct of business in the event of a major disaster is crucial. These documents contain the information necessary to recreate the organization's legal and financial position. Vital records generally represent only a small portion of all records and information maintained by the organization. The records manager will review the vital records program annually. Areas of importance are financial records, employee records, insurance policy information, ownership records, major contracts and agreements, corporate records, and negotiable instruments.

Electronic Records Policy Statement

Each organization's e-mail policy should reflect its own culture and the legal and regulatory framework within which it operates. Developers of the policy must consider factors such as legal issues, records-management retention policies, and information management administration of the e-mail system, along with financial and regulatory issues.

Sample 1: The electronic-mail system is owned by the company, and it is to be used for company business. Occasional use of the system for messages of a personal nature will be treated like any other message. The company desires to

-6-

© Copyright 2008. Ronald L. Hicks, Jr. All Rights Reserved.

respect the right to privacy of its employees and does not monitor electronic mail messages as a routine matter. It does, however, reserve the right to access them, view their contents, and track traffic patterns.

Sample 2: When using e-mail, the message created or used may or may not be a record. When it is designated as a record, it is subject to the records-retention policies of the company. Within the company, each person is responsible for controlling records according to the records-management policies, and when an e-mail message is considered a record, it falls into this category.

Sample 3: Before selecting e-mail as a means for communication or document transmission, users should consider the need for immediacy, formality, accountability, access, security, and permanence. E-mail differs from other forms of communication. It is immediate and informal, similar to a telephone conversation, yet it is more permanent. It is as irrevocable as a hard-copy document, yet easy to duplicate, alter, and distribute.

The City (organization, company, etc.) reserves the right to monitor employee use of e-mail by systems administrators or departmental supervisors. Employees are reminded that e-mail use is provided *primarily* for business purposes and not for personal purposes and that employees cannot expect protection of their personal or business-related e-mail correspondence under privacy laws and regulations.

The City will not monitor e-mail messages as a routine matter. The City will, however, respond to legal processes and fulfill its obligations to third parties. The City will inspect the contents of e-mail messages in the course of an investigation triggered by indications of impropriety or as necessary to locate substantive information that is not more readily available by other means.

Electronic Records Guideline

Retention periods are established for records according to departmental, fiscal, and legal requirements. Each record listed on a records-retention schedule specifies a specific period of time that the record is retained. *This retention applies whether the record is on paper or residing on magnetic or optical media (hard disk, floppy disk, tape, CD, etc.).* Once records have reached their designated time for destruction, they should be destroyed or eliminated from all storage media; that is, file cabinets, inactive storage, magnetic media, backups, etc.

Backup media should be stored in a different location than the computer equipment that is used to create them. Electronic records retained in a backup system follow the same retention as similar paper records listed on a retention schedule.

Drafts generally are not retained and should never be retained longer than the finalized version that becomes the record.

Databases are modified over time through the addition, deletion, or revision of information. Reports may be periodically generated to capture or record the information at a point in time. Records that are in databases may use a retention

period until they are superseded. Once information has been superseded, it is generally lost unless provision is made to save it as a report. Historical data should be archived or deleted according to the department's retention schedule.

Form ILC

Sample Records Retention and Destruction Policy

[COMPANY NAME]

RECORDS RETENTION AND DESTRUCTION POLICY

Adopted by the [Executive][Management] Committee
as of _____, 2004Policy StatementI. INTRODUCTION.

The [Executive][Management] Committee of [COMPANY NAME] (the "Company"), has determined that it is advisable and in the best interests of the Company to implement, administer and maintain a records retention and destruction policy (this "Policy") for the purpose of retaining, organizing and disposing of the various Records (as such term is defined below) in the normal course of business of the Company. As part of the implementation of this Policy, the Company also desires to ensure that it complies with applicable federal and state laws and regulations (collectively, "Laws") relating to the retention and destruction of Records.

A. Benefits from this Policy.

Implementation of this Policy will result in benefits such as:

- Promoting longevity of Records;
- Protecting Records from peril, such as fire, wind, rain, storms, snow and foreseeable and unforeseeable natural and unnatural disasters;
- Safekeeping Records that are necessary to the operations of the Company or which must be preserved as required by Laws;
- Promoting efficiency in storage, organization and Record preservation;
- Reducing costs for storage and retrieval expenses, organizational expenses and insurance coverage on storage facilities;
- Protecting Records from destruction due to damage to a storage facility;
- Reducing spatial problems created by the storage of original documentation;
- Easing the location of Records;

- Promoting the efficient exchange and organization of information throughout the Company;
- Creating efficiencies in the provision of services to the Company's customers;
- Increasing employee productivity through the good faith destruction of Records that are no longer used in or useful to the business of the Company; and
- Providing an efficient mechanism to respond to claims, investigations, audits and lawsuits by third parties, including governmental and various state agencies.

B. Adherence to Policy Guidelines.

The officers, [Executive][Management] Committee members and employees of the Company and the parties identified in this Policy must strictly adhere to the guidelines of this Policy, which may be amended or supplemented from time to time by the [Executive][Management] Committee and/or the Records Retention Committee. **This policy is confidential and proprietary information of the company and shall not be disclosed by the recipient hereof unless such disclosure is first approved in writing by the Records Retention Committee (as such term is defined below).**

C. Statement of Policy.

In light of the introduction set forth above, it shall be the policy of the Company to retain Records which are required: (i) for the effective operation and management of the business of the Company; (ii) to comply with Laws; and (iii) to fulfill the Company's legal and contractual obligations to its customers and the state agencies. Such Records shall be retained for the time periods and in the manner described in this Policy. Further, it shall be the policy of the Company to destroy or discard, at the times and in the manner described in this Policy, those Records that are no longer used in or useful to the business and operations of the Company.

The sections that follow in this Policy are intended to amplify the foregoing statements of policy and to set forth information regarding the responsibility of Company employees to implement and administer this Policy. Any questions about this Policy should be directed to the General Counsel of the Company.

II. COMPANY RECORDS.A. Definition of Records.

The term "Records" means all media, whether written or electronic, containing language, numeric, graphic or other information and that are created,

generated or received by an officer, employee, agent or consultant of the Company in the normal course of the Company's business activities and which are deemed to be considered vital or permanent.

For the purposes of this Policy:

- **“Vital”** means essential to the day-to-day operation and management of a given department of the Company or otherwise required to be retained by Laws; and
- **“Permanent”** means non-essential, but of such value that it may potentially impact the day-to-day activities of the department and, therefore, should not be destroyed or discarded.

B. Locations of Records.

Records may be located or stored in a variety of media. These media include, but are not limited to, correspondence, memoranda, forms, reports, checks, journals, ledgers, legal certificates or instruments, contracts, computer printouts, manuals, drawings, photographs, micro-graphics, tapes, computer disks, voice recordings, voice mails, electronic mail (e-mails), Internet content (including web pages), and any other writings such as those set forth on the Records Retention Schedule, and any and all copies of the same made by any and all means whether made by the author, creator or recipient of the media.

C. Ownership of Company Records.

Records stored on any media of the Company are and shall be the sole property of the Company and are not the property of the individuals creating or receiving them unless otherwise determined by the Company in its sole discretion.

III. RECORDS RETENTION COMMITTEE.

In order to have a centralized mechanism to implement, oversee, administer, update and enforce this Policy, the Company hereby creates a Records Retention Committee (the “Committee”). The composition and duties of the Committee are set forth below.

A. Composition of the Committee.

The Committee shall be comprised of those individuals who are appointed by the [Executive][Management] Committee from time to time, provided, that the General Counsel of the Company and a representative of the Company's Information Technology department shall at all times be members of the Committee. The Committee shall be headed by a chairperson selected by the members of the Committee.

-3-

© Copyright 2008. Ronald L. Hicks, Jr. All Rights Reserved.

B. Responsibilities of the Chairperson of the Committee.

The chairperson of the Committee shall:

- Convene and preside over regular meetings of the Committee;
- Regularly report to the [Executive][Management] Committee regarding the activities of the Committee;
- Ensure that necessary work relating to this Policy is completed on a timely basis and disseminated to the Department Representatives (as such term is defined below) in a proper and efficient manner;
- Hold regular meetings with the Department Representatives to discuss the on-going implementation, administration and enforcement of this Policy;
- Authorize and oversee an annual compliance audit of this Policy;
- Ensure that periodic and formal training programs relating to this Policy are made available to Department Representatives and employees;
- Disseminate to the [Executive][Management] Committee, the other members of the Committee and, if necessary, the Department Representatives, any notifications regarding any special circumstances as may be determined by the General Counsel of the Company (e.g., anticipated claims, investigations, audits or lawsuits) that call for immediate action to retain and preserve certain Records or to otherwise deviate from the guidelines and procedures stated in this Policy or promulgated by the Committee.

C. Responsibilities of the Committee.

The Committee shall implement, administer, monitor, enforce and update this Policy, subject to any directives of the [Executive][Management] Committee relating to Record retention and destruction matters. All record retention and destruction issues and questions shall be first referred to the Committee through the Department Representative under whom the question or issue arises. If the Committee cannot resolve the issue or answer the question, it shall consult with the [Executive][Management] Committee thereon.

In addition, the Committee shall:

- Manage and update the Records Retention Schedule which is attached to this Policy to reflect new classes of Records and to delete classes of Records no longer used by the Company;

-4-

© Copyright 2008. Ronald L. Hicks, Jr. All Rights Reserved.

- Determine the manner and location(s) in which Company Records will be stored; and
- Oversee the destruction of Records which no longer are to be retained, as reflected on the Records Retention Schedule;
- Conduct compliance audits and conduct retention and destruction training programs for Department Representatives and employees.

The Committee is authorized to create and promulgate any and all guidelines and procedures that it deems necessary to implement, administer and monitor this Policy. The [Executive][Management] Committee shall review this Policy and all directives of the Committee on at least an annual basis and, if necessary and after consultation with the Committee, amend or modify this Policy.

IV. DEPARTMENT REPRESENTATIVES.

To assist the Committee in its duties pursuant to this Policy and to ensure that each department within the Company adheres to the requirements set forth herein, the Company will appoint a series of Department Representatives who shall have the duties described below.

A. Department Representatives.

In order to effectively implement, administer and enforce this Policy, each department of the Company shall designate one individual in the department (the "Department Representative") who shall be responsible for identifying, retaining and storing (at such locations as shall be determined from time to time by the Committee) the Records of the department.

B. Responsibilities of the Department Representatives.

Each Department Representative shall:

- Upon the expiration of a retention period for a particular Record or class of Records, the applicable Department Representative shall destroy or cause to be destroyed the relevant Record or class of Records, unless suspension of the destruction of such Record or class of Records has been ordered;
- In connection with the destruction of a Record or class of Records, the Department Representative also shall create, or cause to be created, a reasonably detailed index of the Record(s) which are destroyed, and transmit such index to the General Counsel of the Company;
- Follow any and all legally permitted instructions issued by the General Counsel of the Company, the Executive and

Management Committees of the Company and/or the Committee relating to the suspension of destruction of Records and, if applicable, the marshalling of such Records to ensure preservation thereof;

- Communicate directly with the Committee on issues and questions relating to this Policy unless such Department Representative is not the head of the department, in which case, the Department Representative will first communicate such issues or questions to the head of his or her department for resolution or action. If the head of the department and the Department Representative cannot resolve or act upon the issue or question after consultation, he or she shall consult with the Committee for guidance thereon;
- Administer and monitor compliance with this Policy at the department level, which shall include:
 - Conveying to the individuals in the department the requirements of this Policy;
 - Ensuring that all changes, modifications, amendments or deviations to this Policy are communicated throughout the department;
 - Updating the Committee on the types of Records created or received by the department; and
 - Regularly communicating to the Committee the state of his or her department's compliance with this Policy.

V. SPECIFIC RETENTION AND DESTRUCTION GUIDELINES.

A. E-Mail Retention and Deletion Guidelines.

Recognizing that e-mail is the basis for many instances of communication, whether internally or externally, all e-mails that are not to be saved as Records shall be deleted automatically after six (6) months of delivery to, receipt by or transmission by the Company recipient/sender, and the Company's computer servers shall be configured to automatically delete e-mails in individual mail boxes after the expiration of six (6) months. Back up tapes of electronic mail shall be destroyed or erased when the electronic messages on those tapes are more than six (6) months old.

Each user of the Company's e-mail system is responsible for determining which e-mails should be retained as Records in accordance with their respective department's retention requirements as conveyed and administered by the Department Representative. All e-mails that must be retained pursuant to this Policy are to be retained in compliance with the relevant retention period set forth in the Retention Schedule. The retention requirement may be satisfied by printing and filing a hardcopy of the e-mail and/or by filing an electronic copy in an accessible non-private e-mail folder or computer file on the Company's server.

These preserved Records shall be subject to the other relevant provisions of this Policy relating to Record retention. Automatic archiving or rule functions available within the Company's e-mail system should not be relied upon to save such Records.

B. Electronic Records with Tax Implications.

Pursuant to Revenue Ruling 71-20, the Internal Revenue Service ("IRS") has recognized that computer records meet the requirements for record keeping under the Internal Revenue Code. Revenue Procedure 91-59 specifies that taxpayers utilizing computer records must maintain the computer records in both electronic ("machine sensible") and visible format (paper or microfilm) for the period of time that they are subject to tax audit. A taxpayer may be asked to produce the electronic records in a form that is readable on a current computer system and make that data available to the IRS auditor. For this reason, computer records related to accounting and tax matters should be treated as official Company Records and shall be maintained for the same number of years that non-electronic tax and accounting Records of the Company are retained pursuant to the Retention Schedule.

C. Databases.

Databases consist of a number of files and fields of data that provide useful information to the Company. Typically, databases are modified over time through the addition, deletion or modification of records. Reports are periodically prepared to reflect information from the databases that may be useful for specific purposes. Due to the large volume of information typically maintained in databases, reports rarely reflect "all" of the information found on databases. The Company system provides periodic backups to restore databases in case of accidental erasure or disaster. Any databases that contain tax-related information shall be maintained for the same number of years that electronic and non-electronic tax and accounting Records of the Company are retained pursuant to the Retention Schedule.

Reports from databases that contain non tax-related information, including, but not limited to, mailing lists, customer information, marketing information and product information (the "Non Tax-Related Database") may not reflect the entire content of the Non Tax-Related Database. As such, the electronic format may contain information which is more complete than the written, visible Non Tax-Related Database reports. For this reason, the electronic record of the Non Tax-Related Database shall be the official Company record of the Non Tax-Related Database. The retention period for the tape back up for the Non Tax-Related Database shall be **[one (1) year]** after the Non Tax-Related Database has been superseded. The written, visible reports generated from a Non Tax-Related Database shall be retained for the periods of time set forth in the Retention Schedule.

-7-

© Copyright 2008. Ronald L. Hicks, Jr. All Rights Reserved.

D. Certain Contracts and Other Records Relating Thereto.

The Company has put into place a customized document management database (the "Database"), which contains electronically scanned versions of certain of the Company's contracts and other documents related thereto. Following the scanning of such contracts and on an ongoing basis, the original versions of the contracts and other documents are to be destroyed and the scanned versions shall be the official Company Record of such contracts and other documents.

In connection with the use of the Database, the Company, will implement quality and security controls. The quality controls will ensure the imaged information cannot be fraudulently altered, erased or lost, and will include at least the following:

- Contracts and other documents related thereto will be scanned and checked to ensure that the scanning process is free of human error;
- In connection with the scanning process, the Company employee under whose direction and control the scanning has occurred will provide a certification stating that the duplicate is a correct copy of the original, or of a specific part thereof, as the case may be;
- The scanned documents will be reviewed to ensure they are exact duplicates of the originals. Any images that are not materially exact duplicates (the Database will not display color or grey-scale shown on the original document) of the original document will be deleted and re-scanned;
- Scanned images will be stored in the Database and will contain safeguards that will prevent the scans from being altered electronically after they are saved to the Database.

The security controls will ensure no unauthorized alterations are made to the electronically stored documents. These controls will include both physical security and data security. Security controls will include at least the following:

- Passwords protections to enter the database;
- A mechanism that automatically logs a user out of the Database after the user has not used the Database for a certain period of time;
- Limits on the ability of certain users to access specified applications within the database;
- Limits on the ability of certain users to access specified data/records within the database;

-8-

© Copyright 2008. Ronald L. Hicks, Jr. All Rights Reserved.

- Limits on users' ability to alter data (but users shall not be permitted to alter scanned documents stored in the Database) within the database; and
- Other controls will be implemented as necessary.

E. Guidelines Regarding Destruction of Records.

Any documents destroyed by the Company pursuant to this Policy must be destroyed in good faith and in the regular course of the Company's business. Records residing in the Company's computer system or the database will be permanently deleted upon the expiration of the applicable period set forth on the Retention Schedule. Paper copies of Records shall be shredded and discarded at the expiration of the applicable retention period.

F. Preservation of Records.

In addition to strictly adhering to this Policy, the Company also must preserve all Records (i.e., to suspend destruction thereof) that are reasonably likely to be relevant to present, pending or reasonably foreseeable lawsuits, claims, governmental or other investigations or audits relating to the Company. A lawsuit shall be deemed to be "reasonably foreseeable" if the Company knows or should know the Records are relevant before litigation has been commenced. The General Counsel of the Company shall have the responsibility to disseminate to the Committee and others within the Company, all notifications of present, pending or probable lawsuits, claims, investigations or audits, and will in such instances issue specific instructions with respect to the preservation of such Records. Upon receiving such notifications, the appropriate Department Representatives shall **immediately** cause their respective departments to suspend destruction of all Records pertaining to such lawsuits, claims, investigations or audits until further notification and provide for the gathering/assembly of all relevant documents and delivery to the General Counsel of the Company.

All members of the Committee and all employees and consultants of the Company are to comply fully with all such instructions and directions received from the General Counsel with respect to the preservation of Records and are to direct any questions relating to any such instructions and directions to the General Counsel. In the absence of any specific instructions or directions disseminated by the General Counsel, an employee should retain all Records that he or she reasonably believes may be related to a present, pending or probable lawsuit, claim, investigation or audit. Should an employee receive instructions from, or be directed by, the Committee, a Department Representative or other employee or consultant of the Company to destroy Records after receiving notification from the General Counsel to suspend destruction activities, such employee shall immediately notify the General Counsel of such instructions or directions.

G. Sarbanes-Oxley Act Matters.

The Sarbanes-Oxley Act (the "Act") contains a series of requirements relating to, among other matters, corporate governance. Because of the heightened focus of investors, the applicable regulatory authorities and the public at large on matters relating to corporate responsibility, the Company, the Committee, the Department Representatives and all Company employees must be mindful of the requirements of the Act. To ensure compliance by the Company, its officers, **[Executive][Management]** Committee members and employees, a brief description of applicable provisions of the Act is set forth below, together with specific Records retention requirements relating thereto.

1. CEO and CFO Certifications. The Chief Executive Officer ("CEO") and Chief Financial Officer ("CFO") of the Company are required to provide certain certifications about the Company that is included in the Company's periodic reports (i.e., quarterly and annual reports) filed with the U.S. Securities and Exchange Commission (the "SEC"). These certifications include, among other matters, statements by the CEO and CFO that: (a) to their knowledge, the information presented by the Company contains no material misstatements of fact or omissions of fact that would make the statements made misleading; (b) the financial statements of, and financial information relating to, the Company fairly presents in all material respect the financial condition, results of operations and cash flows of the Company as of and for the periods presented; and (c) they are responsible for establishing, maintaining and evaluating certain procedures for the recordation, processing, summarization and reporting of information relating to the Company for inclusion in periodic reports filed with the SEC. Additionally, the CEO and CFO likely will be required to make further, future certifications relating to the methods of preparation and reliability of the Company's financial statements, the policies and procedures of the Company relating to the accurate and timely recording of transactions and the ability to detect unauthorized activities that could have a material effect on the company's financial statements.

All Records that are developed by the Company in order to enable the CEO and CFO to make the certifications required shall be retained by the Company permanently.

2. Certain Evaluations and Assessments. As part of the aforementioned certifications, the CEO and CFO, as well as other members of the Company's management, must now conduct, or in the future must conduct, evaluations and assessments of: (a) the procedures by which the Company records, processes, summarizes and reports information relating to the Company for inclusion in periodic reports filed with the SEC; and (b) the preparation and reliability of the Company's financial statements, the policies and procedures of the Company relating to the accurate and timely recording of transactions and the ability of the Company to detect unauthorized activities that could have a material

effect on the Company's financial statements. All Records that are developed by the Company in connection with such evaluations and assessments, if any, shall be retained by the Company permanently.

3. Certain Audit Committee Functions. Pursuant to the Act, each public company is required to have a fully independent audit committee of its board of directors, and such audit committee is charged with a variety of responsibilities, including: (a) having the direct responsibility for retaining and compensating an independent, outside auditor; (b) monitoring the independence and competence of the outside auditor; (c) pre-approving audit services and permitted non-audit services by the outside auditor; (d) engaging in periodic communications with the outside auditor; (e) overseeing the internal audit functions of the company; (f) reviewing the company's financial disclosures; (g) establishing procedures for the receipt, retention and treatment of complaints about accounting, auditing and related matters; (h) establishing procedures for the receipt, retention and treatment of confidential and anonymous submission of concerns about questionable auditing or accounting matters from company employees; and (i) monitoring the creation, implementation and adherence to the company's codes of ethics. The Company may be required to have an independent audit committee which is required to perform all or a portion of the foregoing functions. In such event, all Records of such audit committee relating to its required functions pursuant to the Act shall be retained by the Company permanently.

4. Maintenance of Audit Records. The Act and its implementing regulations require an outside auditor of a public company to maintain its work papers and other records relating to an audit or review of a public company's financial statements for a period of seven (7) years. Although this requirement does not apply to a public company itself, the Company should retain all materials provided to an outside auditor in connection with an audit or review of financial statements for a minimum of seven (7) years following the completion of the audit or review to which the materials relate.

5. Internal Investigations Relating to Fraud or Alleged Violations of Securities Laws. In the event that the Company or any of its or their officers engage in an internal investigation of alleged fraud or alleged violations of securities laws, (including, but not limited to, investigations by an audit committee pursuant to its responsibilities set forth above and investigations prompted by an in-house or outside attorney reporting of evidence of the reasonable likelihood of a material violation of securities laws), all Records pertaining to such investigation, the resolution thereof and any remedial measures taken by the Company as a result thereof shall be retained by the Company permanently.

VI. TRAINING PROGRAMS.

The Company will implement a training program for the users, operators and staff covering all stages of this Policy. This training will ensure quality control over the scanning and storage of imaged documents, the preservation and destruction of other electronic Records and the preservation and destruction of paper Records. The training program will cover quality and security controls, the importance of adherence to this Policy and proper methods for Record destruction. The Company will regularly update the training materials to reflect any changes in this Policy.

VII. PENALTIES / SANCTIONS FOR NON-COMPLIANCE.

All employees of the Company must adhere to this Policy and the guidelines and procedures issued by the Committee from time to time. If an employee fails to do so, he or she may be subject to penalties/sanctions levied by the Company in addition to any penalties prescribed by Laws, including, without limitation, §802 of the Act, which makes it a crime, punishable by up to twenty (20) years in prison, for any person to alter, destroy or falsify documents with the intent to obstruct the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any bankruptcy case.

VIII. RETENTION SCHEDULE

See attached.

**Form III
Sample Record/Information Retention Schedule**

RECORD SERIES TITLE/ASSET NAME	COMPANY RETENTION PERIOD	ASSET OWNER DEPARTMENT	Statute/Regulation & Retention Period	Comments
1099's	7 years	Accounts Payable	SEC - 17 CFR 257.2 12c 6 yrs	No change recommended
401(K) Contribution Report and Payments	6 years	Payroll	SEC - 17 CFR 257.2 16a 6 yrs ERISA - 29 U.S.C. §1027 6 yrs, but may need to be retained longer if the records contain information relevant to a determination of an individual's benefit entitlements under a pension plan	No change recommended
Accident Investigations	6 years	Distribution Safety	OSHA - 29 CFR 1904.33 5 yrs + current yr	No change recommended
Accounts Receivable Invoices	3 years after settlement	Corporate Accounting	SEC - 17 CFR 257.2 9b 3 yrs after settlement	No change recommended
Accounts Receivable Register	3 years after settlement	Corporate Accounting	SEC - 17 CFR 257.2 9a 3 yrs after settlement	No change recommended
Ad Agency Contracts	All such contracts except those governed by Ohio law: 6 years after cancellation or expiration. For contracts governed by Ohio law, 15 years after cancellation or expiration.	Marketing Communications	SEC-17 CFR 257.2 5a 6 yrs after cancellation or expiration State statute of limitations for breach of contract actions	Recommend 15 years following the cancellation or termination of agreements governed by Ohio law, as the Ohio Statute of Limitations on breach of written contracts is 15 years. Recommend 6 years following the cancellation or termination of the agreements for all other jurisdictions, as that is the longest statute of limitations for breach of contract actions made outside of Ohio.
Advertisements	6 years	Marketing Communications	SEC - 17 CFR 257.2 27a 6 yrs after date of publication	No change recommended

RECORD SERIES TITLE/ASSET NAME	COMPANY RETENTION PERIOD	ASSET OWNER DEPARTMENT	Statute/Regulation & Retention Period	Comments
Advertising Archives	Life of company	Marketing Communications	SEC - 17 CFR 257.2 27a 6 yrs after date of publication	No change recommended
Affirmative Action Plan & Reporting	15 years	Employment & Diversity	OFCCP - 41 CFR 60-2.32 2 yrs	No change recommended
Annual Benefits Enrollment Files	6 years after termination	Compensation & Benefits	SEC - 17 CFR 257.2 17c 6 yrs after termination of program ERISA - 29 U.S.C.A. 1059(a)(1)	No change recommended
Annual Year-end Reports	10 years	Accounts Payable	Department Policy	No change recommended
Applications for Employment (Including Resumes)	3 years	Employment & Diversity	OFCCP - 41 CFR 60-1.12 2 yrs FLSA - 29 CFR 516.2(a) 3 yrs ADEA - 29 CFR 1627.3(b)(1) 1 yr Title VII - 29 CFR 1602.14 1 yr ADA - 29 CFR 1602.14 1 yr	No change recommended
Audit Reports & Memos	7 years	Audit Services	SEC - 17 CFR 257.2 25b 6 yrs after date of report SEC - 17 CFR 210.2-06 7 yrs	Recommend changing to 7 years; pursuant to Reg. 210.2-06, auditors are required to keep audit records for 7 years; the Company should maintain information for a like period to be able to confirm auditors' records.
Audit Workpaper Files	7 years	Audit Services	SEC-17 CFR 257.2 25b 6 yrs after date of report SEC - 17 CFR 210.2-06 7 yrs	Recommend changing to 7 years; pursuant to Reg. 210.2-06, auditors are required to keep audit records for 7 years; the Company should maintain information for a like period to be able to confirm auditors' records.
Budget Forecasting (Interest)	6 years	Corporate Finance	SEC-17 CFR 257.2 26 6 yrs	No change recommended
Budget Information for General Users	2 years	Corporate Budgets	Department Policy	No change recommended

RECORD SERIES TITLE/ASSET NAME	COMPANY RETENTION PERIOD	ASSET OWNER DEPARTMENT	Statute/Regulation & Retention Period	Comments
Budget Reports for Operations & Customer Service Divisions	6 years	Field & Management Support	SEC CFR 257.2 26 6 yrs	No change recommended
Budget Variance Reports	6 years	Field & Management Support	Department Policy	No change recommended
Business Plan	10 years	Business Development	SEC-17 CFR 257.2 26 6 yrs	No change recommended
Career Development Reports	Life of company	Training	ADEA - 29 CFR 1627.3b1 1 yr Title VII - 29 CFR 1602.14 1 yr ADA - 29 CFR 1602.14 1 yr	No change recommended
Cash Disbursements Detail	6 years	Accounts Payable	SEC-17 CFR 257.2 15a Destroy at option after audit	No change recommended
Cash Reports	3 years	Billing Services	SEC-17 CFR 257.2 15a Destroy at option after audit	No change recommended
Chart of Accounts	50 years	Corporate Accounting	SEC-17 CFR 257.2 7c Destroy when superseded	No change recommended
Company Financing	Life of company	Corporate Secretary	SEC-17 CFR 257.2 1h & 1i 3 yrs after redemption	No change recommended
Contracts	All such contracts except those governed by Ohio law: 6 years after cancellation or expiration. For contracts governed by Ohio law, 15 years after cancellation or expiration.	Purchasing	SEC-17 CFR 257.2 5a 6 yrs after cancellation or expiration State statute of limitations for breach of contract actions	Recommend 15 years following the cancellation or termination of agreements governed by Ohio law, as the Ohio Statute of Limitations on breach of written contracts is 15 years. Recommend 6 years following the cancellation or termination of the agreements for all other jurisdictions, as that is the longest statute of limitations for breach of contract actions made outside of Ohio.

RECORD SERIES TITLE/ASSET NAME	COMPANY RETENTION PERIOD	ASSET OWNER DEPARTMENT	Statute/Regulation & Retention Period	Comments
Contracts & Agreements	All such contracts except those governed by Ohio law: 6 years after cancellation or expiration. For contracts governed by Ohio law, 15 years after cancellation or expiration.	Records Management	SEC-17 CFR 257.2 5a 6 yrs after cancellation or expiration State statute of limitations for breach of contract actions	Recommend 15 years following the cancellation or termination of agreements governed by Ohio law, as the Ohio Statute of Limitations on breach of written contracts is 15 years. Recommend 6 years following the cancellation or termination of the agreements for all other jurisdictions, as that is the longest statute of limitations for breach of contract actions made outside of Ohio.
Corporate Executive Records	Life of company	Corporate Secretary	SEC-17 CFR 257.2 4a(1) Life of corporation	No change recommended
Corporate Finance Calendar	3 years	Corporate Finance	Department Policy	No change recommended
Customer Call Center Correspondence	5 years	Customer Services	Department Policy	No change recommended
Customer Complaint Files	3 years	Regulatory Affairs	OH - 4901:1-21-08 1 yr TX - 17.152(a)(5), 17.153(a-c), 25.491(b)(1-2) not less than 24 months NJ - 14:4-2.6(d)(4) 3 years MD - 7-507(m) no duration specified DE - Reg. 10 800 049V(2)(d) 3 yrs	Duration of the complaint or 3 years, whichever is longer because Maryland's statute of limitations for actions brought on contracts is 3 years
Customer's Written Consent to the Release of Customer Information	3 years	TBD	DC Order No. 11796 indefinitely NY - Case 98-M-1343 2 yrs	Recommend 3 years because that is the statute of limitations for contracts under District of Columbia law

RECORD SERIES TITLE/ASSET NAME	COMPANY RETENTION PERIOD	ASSET OWNER DEPARTMENT	Statute/Regulation & Retention Period	Comments
Customer Letters	3 years	Product Management	NJ - 14.4-2.6(d)(4) 3 yrs NY - Case 98-M-1343 2 yrs TX - 17.151(b)(1-4) 24 months DE - Reg. 10 800 049III(11) - 2 yrs	Recommend 3 years
Disciplinary Files (Results & Actions)	Life of company	HR Administration	SEC-257.2 17a 3 yrs after termination of employment ADEA-29 CFR 1627.3(b)(1) 3 yrs Title VII - 29 CFR 1602.14 1 yr ADA - 29 CFR 1602.14 1 yr	No change recommended
Disaster Recovery Plans	Retain until superseded	Security	Department Policy	No change recommended
Drug Testing Records	5 years	Safety	ADEA - 29 CFR 1627.3(b)(1) 1 yr Title VII - 29 CFR 1602.14 1 yr ADA - 29 CFR 1602.14 1 yr	No change recommended
Drugs & Alcohol Letters of Understanding	Life of company	HR Administration	ADEA - 29 CFR 1627.3b(1) 1 yr Title VII - 29 CFR 1602.14 1 yr ADA - 29 CFR 1602.14 1 yr	No change recommended
Employee Medical Charts & Records	30 years after termination of employment	Medical	OSHA - 29 CFR 1910.1020d(1) 30 yrs after termination of employment	No change recommended

RECORD SERIES TITLE/ASSET NAME	COMPANY RETENTION PERIOD	ASSET OWNER DEPARTMENT	Statute/Regulation & Retention Period	Comments
Employee Personnel Files (All)	5 years after termination of employment or until the final disposition of any employee complaint	Maintenance	SEC - 17 CFR 257.2 17a 3 yrs after termination of employment ADEA - 29 CFR 1627.3 b(1) 1 yr from the date of the personnel action to which the records relate Title VII - 29 CFR 1602.14 1 yr from the date the record was made or the date the action occurred, whichever was later ADA - 29 CFR 1602.14 1 yr PA - Admin. Code 16 ADC 41.81 120 days PA - Admin. Code 16 ADC 41.82 until the final disposition of any employee complaint (maintain employee records and the records of any employees holding similar positions to position of complainant) CT - 38-128b 1 yr	Recommend maintaining the records five years or until disposition of any employee complaint
Family Medical Leave Act (FMLA)	3 years	Medical	FMLA - 29 C.F.R. 825.500(c)(1-7) 3 yrs	No change recommended
Floor Plans	1 year for department copy	Facilities Maintenance & Management	Department Policy	No change recommended
Garnishments, Levies, Wage Assignments, Etc.	5 years after file is closed	Law	Department Policy FLSA - 29 CFR 516.6(a), (c) 2 yrs	No change recommended

RECORD SERIES TITLE/ASSET NAME	COMPANY RETENTION PERIOD	ASSET OWNER DEPARTMENT	Statute/Regulation & Retention Period	Comments
General Litigation: Including Personal Injury and Property Damage	5 years after file is closed	Law	Department Policy	No change recommended
HR Investigations	Life of company	HR Administration	Department Policy ADEA - 29 CFR 1627.3(b)(1) 3 yrs Title VII - 29 CFR 1602.14 1 yr ADA - 29 CFR 1602.14 1 yr PA - Admin. Code 16 ADC 41.81 120 days	No change recommended
Job Descriptions (Management)	Life of company	Compensation & Benefits	ADEA - 29 CFR 1627.3b(1) 1 yr Title VII - 29 CFR 1602.14 1 yr ADA - 29 CFR 1602.14 1 yr PA - Admin. Code 16 ADC 41.81 120 days	No change recommended
Job Interview Notes	5 years	Employment & Diversity	OFCCP - 41 CFR 60-1.12 2 yrs ADEA - 29 CFR 1627.3b(1) 1 yr Title VII - 29 CFR 1602.14 1 yr ADA - 29 CFR 1602.14 1 yr PA - Admin. Code 16 ADC 41.81 120 days	No change recommended
Labor/Employment – Corporate Personnel Records	5 years after termination of employment	Law	SEC-17 CFR 257.2 17(a) 3 yrs after termination of employment ADEA - 29 CFR 1627.3b(1) 1 yr Title VII - 29 CFR 1602.14 1 yr ADA - 29 CFR 1602.14 1 yr PA - Admin. Code 16 ADC 41.81 120 days	No change recommended

RECORD SERIES TITLE/ASSET NAME	COMPANY RETENTION PERIOD	ASSET OWNER DEPARTMENT	Statute/Regulation & Retention Period	Comments
Labor/Employment – Investigative Files/Reports	5 years after termination of employment	Law	SEC-17 CFR 257.2 17(a) 3 yrs after termination of employment ADEA - 29 CFR 1627.3b(1) 1 yr Title VII - 29 CFR 1602.14 1 yr ADA - 29 CFR 1602 PA - Admin. Code 16 ADC 41.81 120 days	No change recommended
Labor/Employment – Job Elimination Letters/Information	5 years after termination of employment	Law	SEC-17 CFR 257.2 17(a) 3 yrs after termination of employment ADEA - 29 CFR 1627.3b(1) 1 yr Title VII - 29 CFR 1602.14 1 yr ADA - 29 CFR 1602.14 1 yr PA - Admin. Code 16 ADC 41.81 120 days	No change recommended
Labor/Employment – Severance/Settlement Agreements & Databases/Charts	All such contracts except those governed by Ohio law: 6 years after cancellation or expiration. For contracts governed by Ohio law, 15 years after cancellation or expiration.	Law	SEC-17 CFR 257.2 17(a) 3 yrs after termination of employment ADEA - 29 CFR 1627.3b(1) 1 yr Title VII - 29 CFR 1602.14 1 yr ADA - 29 CFR 1602.14 1 yr PA - Admin. Code 16 ADC 41.81 120 days State statute of limitations for breach of contract actions	Recommend 15 years following the cancellation or termination of agreements governed by Ohio law, as the Ohio Statute of Limitations on breach of written contracts is 15 years. Recommend 6 years following the cancellation or termination of the agreements for all other jurisdictions, as that is the longest statute of limitations for breach of contract actions made outside of Ohio.

Form IV.A(1)

Sample Preservation Notice to Employees/Agents**PLEASE READ THIS IMPORTANT
DOCUMENT PRESERVATION NOTICE****ATTORNEY-CLIENT PRIVILEGED AND CONFIDENTIAL**

Preservation Notice relating to:

Company A, Inc. v. Corporation B, Inc.**(Case No. 1234)**

and

Corporation B, Inc. v. Company A, Inc. and Company C, Inc.**(Case No. 06-1574)**

This document preservation notice concerns a lawsuit initiated by Company A ("A") against Corporation B ("B") generally relating to the Joint Development and License Agreement between A and B. A filed against B in federal court in Maryland, however that case has been transferred to the United States District Court for the Southern District of California. On the same day the Maryland case was transferred, B filed its own lawsuit against A and Company C alleging that, among other things, A and C stole trade secrets from B. We believe that the two cases will be consolidated but at present, there are two separate actions.

We believe that you may have records or information relating to these cases. This memo contains **important directions about preserving relevant records** and information. Make sure you understand them. This direction supersedes all record retention policies—even documents that would ordinarily be destroyed as a part of our routine records management program, if related, must be preserved. If you have any questions, call me or our outside counsel, John Smith at Law Firm.

It is very important that you retain all records that contain any information relating to these matters. These records must be retained until you are informed by Legal that the matters have been concluded and the records no longer need to be retained.

Records means anything that stores information --

in any medium – paper, electronic, video and audiotapes, etc., including e-mails and all other electronic files (see below).

in any form – handwritten or typed, draft or final, desk or electronic calendars and phone slip notes created at any time, including records you create in the future, wherever maintained, whether on your computer, in your office, in departmental files, in a home office, in your car, or elsewhere.

You must retain all and any records that contain information that has any connection whatsoever to either matter or to any of the issues summarized below. Even if the relevant information is only a small part of the record, e.g., a bullet point in a business or strategic plan, you must retain the entire document. If you are uncertain about whether a record **relates to** this matter, retain it - you may also check with me to determine whether you need to retain it.

Specifically, these matters involve the following key elements:

In February 20__, A and B entered an agreement to work together to develop an Application Specific Integrated Circuit ("ASIC") for use in a communications technology product. The relationship broke down and A and B now dispute what their rights are to certain intellectual property and the ASIC.

B alleges that Company C violated a Nondisclosure Agreement that existed between B and A when C allegedly continued to work with A to develop the ASIC. B alleges it was excluded from any further dealings.

B is also accusing A of trade secret misappropriation because C and A allegedly continued to work together after termination of the JDA to develop the ASIC. B alleges that its trade secrets and intellectual property were central to the development of the ASIC by A and C.

You must retain any record that relates to the foregoing topics. This list of topics may be modified or supplemented periodically once outside counsel and in-house counsel have determined the kinds of documents they're looking for.

If the specified records exist in paper form, you must keep them, without alteration, organized in the way that you would normally keep them for business purposes (for example, if you usually file them in folders, continue to do so). Unless your home office is your principal office, the records should be kept at a company location within the control of you and/or your department. Electronic records should generally be kept in electronic form. To the extent that any such records involve data that continually changes you may satisfy the requirement by printing and retaining a monthly summary. If electronic files were created which you

did not retain a copy of, please let me know and we will determine how best to recover these electronic documents (including emails received and sent).

If you believe this memo should be provided to anyone else, please let me know as soon as possible. If you are aware of other individuals who are not on the distribution list who might have documents relating to this matter, including outside contractors or vendors, please let me know and I will send them a copy of this memo. Please do not send the memo yourself; I want to keep a record of all individuals to whom the memo is sent.

Please notify me promptly in the event that you are changing jobs within the Company or are leaving the Company. I will make arrangements with you to appropriately preserve documents you are maintaining pursuant to this notice. Nothing in this notice shall be deemed an admission of relevancy or agreement to produce documents in connection with the pending litigation. The Company hereby reserves the right to object to production of any and all documents covered by this notice on the basis of relevancy, privilege or any other reasonable grounds. Set forth below are some important reminders about document creation and inquires from third parties regarding these matters. Thank you for your important cooperation in these matters. Again, if you have any questions about these matters, please call _____.

DOCUMENT CREATION REMINDERS

1. Keep in mind that all documents and records that you prepare may be provided to opposing counsel. Like all documents and records that already exist, we may be required to produce any new documents to the attorneys representing our opponents. You should keep this in mind as you prepare documents and as you make decisions about whether or not documents need to be prepared. In general, try to limit any documents you prepare that may be relevant to this case to statements of fact, rather than opinions. Also, be especially conscious of the possibility for statements in documents to be taken out of context.

2. Do not pass on legal opinions to other people, including other people within the Company. The Attorney/Client Privilege protects us from being required to disclose the legal advice we provide to you. However, this privilege only protects confidential communications between lawyers and clients; so, if you pass that advice on to another person, it could cause us to lose the privilege. Although any improper sharing of legal advice, even verbally, could cause us to lose the privilege, it is particularly important that you do not communicate any legal advice in writing (including e-mail). If someone else within the Company needs to hear the advice, please ask a lawyer to provide that advice directly. If there is a need to create a document, including e-mail, that comments on the case or the issues in the case, please ensure that it is at least directed to a Company attorney in the "to" line and is marked as a confidential and privileged communication.

3. Do not discuss this case with anyone outside of the Company, especially the media. You know not to discuss the Company's confidential information with individuals outside of the Company. Information relating to this case is confidential and should not be discussed with anyone who does not have a need to know it. This includes customers, brokers, suppliers, external manufacturers, employees and especially the media. If anyone asks you for information, you should tell them that we have no comment. If you receive media inquiries, refer them to Corporate Affairs. If anyone from the opposing side contacts you to discuss this matter, please do not share any information and contact me immediately.

Form IV.A(2)

Sample Preservation Notice to Employees/Agents

PLEASE READ THIS IMPORTANT DOCUMENT PRESERVATION NOTICE

ATTORNEY-CLIENT PRIVILEGED AND CONFIDENTIAL

[Press F11 then press ALT D FOR DATE]

[Press F11, Type Employee or Agent Name]"

[Press F11, Type Address]

RE: [Press F11, Identify Litigation matter]"

Document & Data Preservation Notice

Dear [Press F11, Type Salutation]:

The Company has received notice of the above-referenced matter (the "Claim"). In light of this notice, the Company requires your assistance in preserving all paper records and electronically stored data that are relevant to this matter and are in your possession, custody or control.

Electronically stored data is an important and irreplaceable source of discovery and/or evidence in this matter. Notice of the above lawsuit requires preservation of all information from the Company's paper records and computer systems, removable electronic media, and other locations relating to the Claim. For purposes of this Notice, this information includes, but is not limited to, all text files (including word processing documents), presentation files (such as PowerPoint), spread sheets, e-mail files and information concerning e-mail files (including logs of e-mail history and usage, header information, and deleted files), Internet history files and preferences, graphical image files in any format, databases, calendar and scheduling information, task lists, journals, telephone logs, contact managers, computer system activity logs, and all file fragments and backup files containing electronic data.

Employees must take every reasonable step to preserve this information until further notice. Specifically, you are instructed not to destroy, disable, erase, encrypt, alter, or otherwise make unavailable any paper record or electronic evidence relevant to the Claim, and you are further instructed to take reasonable efforts to preserve such information. ***Failure to do so could result in extreme penalties against the Company.***

To provide the assistance requested by this Notice, you are instructed by way of example and not limitation, to do the following:

- Preserve all paper records and data storage backup files (*i.e.*, not overwrite any previously existing backups);
- Preserve and retain all paper records and electronic data generated or received by you and other employees who may have personal knowledge of the facts involved in the Claim, including but not limited to those of _____, _____, and _____;
- Refrain from operating (or removing or altering fixed or external drives and media attached thereto) any stand-alone personal computers, network workstations, notebook and/or laptop computers, cell phones, PDAs or Smartphones, BlackBerrys or other similar computing devices that are reasonably thought to have data related to the Claim, including but not limited to those operated by _____, _____, and _____;
- Preserve and retain all data from servers and networking equipment logging network access activity and system authentication;
- Preserve and retain all electronic data in any format, media, or location relating to the Claim, including data on floppy disks, Zip disks, CD-ROMs, CD-RWs, DVDs, DVD-RWs, tapes, PDAs, cell phones, memory cards/sticks, or digital copiers;
- Prevent employees from deleting or overwriting any electronic data related to the Claim; and
- Take such other security measures, including, but not limited to, restricting physical and electronic access to all electronically stored data directly or indirectly related to the Claim.

To facilitate the preservation of data, the Company has engaged [Press F11, Type Contact Name]" to forensically acquire the hard drives and other media that are in your possession, custody or control and that may contain electronic data related to the Claim. Kindly call [Press F11, Type Contact Name]" at [Press F11, Type Phone Number]" upon receipt of this letter so that we may arrange the details of the acquisition.

If this correspondence and the request made herein are in any respect unclear, please contact [Press F11, Type Contact Name]" at [Press F11, Type Phone Number]" .

[Press F11, Type Closing]

Form IV.B

Sample Preservation Notice to Adverse or Third Parties

[Press F11 then press ALT D FOR DATE]

[Press F11, Type Recipient]

[Press F11, Type Address]

RE: [Press F11, Identify Litigation matter]"

Document & Data Preservation Notice

Dear [Press F11, Type Salutation]:

By this letter, you are hereby given notice of the above-referenced matter (the "Claim"). In connection with such Claim, you may have in your possession, custody, or control documents, information, and electronically or digitally stored information relevant to the Claim. Also, you and/or your agents and employees may have knowledge of facts relevant to the Claim. Consequently, this letter serves not only as notice of the Claim, but also as notice not to destroy, conceal, or alter any paper or electronic files and other data generated by you or your employees and/or stored on your company's computers, storage media (e.g., hard disks, floppy disks, backup tapes), or any other electronic data, such as voice mail. Your failure to comply with this notice can result in both severe sanctions being imposed by the Court and liability in tort for spoliation of evidence or potential evidence.

Through discovery, we expect to obtain from you a number of documents and things, including files stored on your company's computers and storage media. In order to avoid spoliation, you will need to provide the data requested on the original media. Do not reuse any media to provide this data.

Electronic documents and the storage media on which they reside contain relevant, discoverable information beyond what may be found in printed documents. Therefore, even where a paper copy exists, we will seek all documents in their electronic form along with information about those documents contained on the media. Also, we will seek paper printouts of only those documents that contain unique information after they were printed out (such as paper documents containing handwriting, signatures, marginalia, drawings, annotations, highlighting and redactions) along with any paper documents for which no corresponding electronic files exist.

Our discovery requests will ask for certain data on the hard disks, floppy disks and backup media used in your company's computers, some of which data are not readily available to an ordinary computer user, such as "deleted" files and "file fragments." As you may know, although a user may "erase" or "delete" a file, all

that is really erased is a reference to that file in a table on the hard disk; unless overwritten with new data, a "deleted" file can be as intact on the disk as any "active" file you would see in a directory listing.

Accordingly, electronic data and storage media that may be subject to our discovery requests and that you are obligated to maintain and not alter or destroy, include but are not limited to the following:

Description of Files and File Types Sought:

All digital or analog electronic files, including "deleted" files and file fragments, stored in machine-readable format on magnetic, optical, or other storage media, including the hard drives or floppy disks used by your company's computers and their backup media (e.g., other hard drives, backup tapes, floppies, JAZ cartridges, CD-ROMs) or otherwise, regardless of whether such files have been reduced to paper printouts. More specifically, you are to preserve all of your e-mails, both sent and received, whether internally or externally; all word-processed files, including drafts and revisions; all spreadsheets, including drafts and revisions; all databases; all CAD (computer-aided design) files, including drafts and revisions; all presentation data or slide shows produced by presentation software (such as Microsoft PowerPoint); all graphs, charts, and other data produced by project management software (such as Microsoft Project); all data generated by calendaring, task management, and personal information management (PIM) software (such as Microsoft Outlook or Lotus Notes); all data created with the use of personal data assistants (PDAs), such as PalmPilot, iPaq or other Windows CE, Pocket PC, or Windows Mobile devices; all data created with the use of document-management software; all data created with the use of paper and electronic mail logging and routing software; all Internet and Web-browser-generated history files, caches, and "cookies" files generated at the workstation of each employee and/or agent in your company's employ and on any and all backup storage media; and any and all other files generated by users through the use of computers and/or telecommunications, including but not limited to voice mail.

Further, you are to preserve any log or logs of network use by employees or otherwise, whether kept in paper or electronic form, and to preserve all copies of your backup tapes and the software necessary to reconstruct the data on those tapes, so there can be made a complete, bit-by-bit "mirror" evidentiary image copy of the storage media of each and every personal computer (and/or workstation) and network server in your control and custody, as well as image copies of all hard drives retained by you and no longer in service, but in use at any time from _____ to the present.

You are also not to pack, compress, purge or otherwise dispose of files and parts of files unless a true and correct copy of such files is made.

You are to preserve and not destroy all passwords, decryption procedures (including, if necessary, the software to decrypt the files); network access codes, ID names, manuals, tutorials, written instructions, decompression or reconstruction software, and any and all other information and things necessary to

access, view and (if necessary) reconstruct the electronic data we will request through discovery.

Documents Subject to Preservation Notice:

1. **Business Records:** [All documents and information about documents containing backup and/or archive policy and/or procedure, document retention policy, names of backup and/or archive software, names and addresses of any offsite storage provider.]

a. All e-mail and information about e-mail (including message contents, header information and logs of e-mail system usage) (sent or received) by the following persons:

[List names, job titles]

b. All other e-mail and information about e-mail (including message contents, header information and logs of e-mail system usage) containing information about or related to:

[Insert detail]

c. All databases (including all records and fields and structural information in such databases), containing any reference to and/or information about or related to:

[Insert detail]

d. All logs of activity (both in paper and electronic formats) on computer systems and networks that have or may have been used to process or store electronic data containing information about or related to:

[Insert detail]

e. All word processing files, including prior drafts, "deleted" files, and file fragments, containing information about or related to:

[Insert detail]

f. With regard to electronic data created by application programs that process financial, accounting and billing information, all electronic data files, including prior drafts, "deleted" files, and file fragments, containing information about or related to:

[Insert detail]

g. All files, including prior drafts, "deleted" files, and file fragments, containing information from electronic calendars and scheduling programs regarding or related to:

[Insert detail]

h. All electronic data files, including prior drafts, "deleted," files and file fragments about or related to:

[Insert detail]

2. **Online Data Storage on Mainframes and Minicomputers:** With regard to online storage and/or direct access storage devices attached to your company's mainframe computers and/or minicomputers: they are not to modify or delete any electronic data files, "deleted" files and file fragments existing at the time of this letter's delivery, which meet the definitions set forth in this letter, unless a true and correct copy of each such electronic data file has been made and steps have been taken to ensure that such a copy will be preserved and accessible for purposes of this litigation.
3. **Offline Data Storage, Backups and Archives, Floppy Diskettes, Tapes, and Other Removable Electronic Media:** With regard to all electronic media used for offline storage, including magnetic tapes and cartridges and other media that, at the time of this letter's delivery, contained any electronic data meeting the criteria listed in paragraph 1 above: You are to stop any activity that may result in the loss of such electronic data, including rotation, destruction, overwriting and/or erasure of such media in whole or in part. This request is intended to cover all removable electronic media used for data storage in connection with their computer systems, including magnetic tapes and cartridges, magneto-optical disks, floppy diskettes, and all other media, whether used with personal computers, minicomputers, or mainframes or other computers, and whether containing backup and/or archive data sets and other electronic data, for all of their computer systems.
4. **Replacement of Data Storage Devices:** You are not to dispose of any electronic data storage devices and/or media that may be replaced due to failure and/or upgrade and/or other reasons that may contain electronic data meeting the criteria listed in paragraph 1 above.
5. **Fixed Drives on Stand-Alone Personal Computers and Network Workstations:** With regard to electronic data meeting the criteria listed in paragraph 1 above, which existed on fixed drives attached to stand-alone microcomputers and/or network workstations at the time of this letter's delivery: You are not to alter, erase, wipe, or scrub such electronic data, and not to perform other procedures (such as data compression and disk defragmentation or optimization routines) that may impact such data, unless a true and correct copy has been made of such active files and of completely restored versions of such deleted electronic files and file fragments, copies have been made of all directory listings (including hidden files) for all directories and subdirectories containing such files, and arrangements have been made to preserve copies during the pendency of this litigation.
6. **Programs and Utilities:** You are to preserve copies of all application programs and utilities, which may be used to process electronic data covered by this letter.
7. **Log of System Modifications:** You are to maintain an activity log to document modifications made to any electronic data processing system that may affect the system's capability to process any electronic data meeting the

criteria listed in paragraph 1 above, regardless of whether such modifications were made by employees, contractors, vendors and/or any other third parties.

8. **Personal Computers, PDAs, Cell Phones, Voice Mail And Other Devices Used by Your Employees and/or Their Secretaries and Assistants:** The following steps should immediately be taken in regard to all personal computers, PDAs, cell phones, voice mail and other devices used by your employees and/or their secretaries and assistants.
- a. As to fixed drives attached to such computers: (i) a true and correct copy is to be made of all electronic data on such fixed drives relating to this matter, including all active files and completely restored versions of all deleted electronic files and file fragments; (ii) full directory listings (including hidden files) for all directories and subdirectories (including hidden directories) on such fixed drives should be written; and (iii) such copies and listings are to be preserved until this matter reaches its final resolution.
 - b. All floppy diskettes, magnetic tapes and cartridges, and other media used in connection with such computers prior to the date of delivery of this letter containing any electronic data relating to this matter are to be collected and put into storage for the duration of this lawsuit.
9. **Evidence Created Subsequent to This Letter:** With regard to electronic data created subsequent to the date of delivery of this letter, relevant evidence is not to be destroyed and you are to take whatever steps are appropriate to avoid destruction of evidence.

To assure that your obligation to preserve documents and things will be met, please forward a copy of this letter to all persons and entities with custodial responsibility for the items referred to in this letter. This request shall remain in effect until further written notice is received from the undersigned.

[Press F11, Type Closing]

Form IV.C

Sample Preservation Notice to Opposing Counsel

[Press F11 then press ALT D FOR DATE]

[Press F11, Type Recipient]

[Press F11, Type Address]

RE: [Press F11, Identify Litigation matter]"

Document & Data Preservation Notice

Dear [Press F11, Type Salutation]:

By this letter, you and your client are hereby given notice not to destroy, conceal, or alter any paper or electronic files and other data generated by you or your employees and/or stored on your company's computers, storage media (e.g., hard disks, floppy disks, backup tapes), or any other electronic data, such as voice mail. As you know, your client's failure to comply with this notice can result in both severe sanctions being imposed by the Court and liability in tort for spoliation of evidence or potential evidence.

Through discovery, we expect to obtain from you and your client a number of documents and things, including files stored on your client's computers and storage media. In order to avoid spoliation, you and your client will need to provide the data requested on the original media. Do not reuse any media to provide this data.

Electronic documents and the storage media on which they reside contain relevant, discoverable information beyond what may be found in printed documents. Therefore, even where a paper copy exists, we will seek all documents in their electronic form along with information about those documents contained on the media. Also, we will seek paper printouts of only those documents that contain unique information after they were printed out (such as paper documents containing handwriting, signatures, marginalia, drawings, annotations, highlighting and redactions) along with any paper documents for which no corresponding electronic files exist.

Our discovery requests will ask for certain data on the hard disks, floppy disks and backup media used in your client's computers, some of which data are not readily available to an ordinary computer user, such as "deleted" files and "file fragments." As you may know, although a user may "erase" or "delete" a file, all that is really erased is a reference to that file in a table on the hard disk; unless overwritten with new data, a "deleted" file can be as intact on the disk as any "active" file you would see in a directory listing.

Accordingly, electronic data and storage media that may be subject to our discovery requests and that your client is obligated to maintain and not alter or destroy, include but are not limited to the following:

Description of Files and File Types Sought:

All digital or analog electronic files, including "deleted" files and file fragments, stored in machine-readable format on magnetic, optical, or other storage media, including the hard drives or floppy disks used by your company's computers and their backup media (e.g., other hard drives, backup tapes, floppies, JAZ cartridges, CD-ROMs) or otherwise, regardless of whether such files have been reduced to paper printouts. More specifically, Your client is to preserve all of your e-mails, both sent and received, whether internally or externally; all word-processed files, including drafts and revisions; all spreadsheets, including drafts and revisions; all databases; all CAD (computer-aided design) files, including drafts and revisions; all presentation data or slide shows produced by presentation software (such as Microsoft PowerPoint); all graphs, charts, and other data produced by project management software (such as Microsoft Project); all data generated by calendaring, task management, and personal information management (PIM) software (such as Microsoft Outlook or Lotus Notes); all data created with the use of personal data assistants (PDAs), such as PalmPilot, iPaq or other Windows CE, Pocket PC, or Windows Mobile devices; all data created with the use of document-management software; all data created with the use of paper and electronic mail logging and routing software; all Internet and Web-browser-generated history files, caches, and "cookies" files generated at the workstation of each employee and/or agent in your company's employ and on any and all backup storage media; and any and all other files generated by users through the use of computers and/or telecommunications, including but not limited to voice mail.

Further, your client is to preserve any log or logs of network use by employees or otherwise, whether kept in paper or electronic form, and to preserve all copies of your backup tapes and the software necessary to reconstruct the data on those tapes, so there can be made a complete, bit-by-bit "mirror" evidentiary image copy of the storage media of each and every personal computer (and/or workstation) and network server in your control and custody, as well as image copies of all hard drives retained by you and no longer in service, but in use at any time from _____ to the present.

Your client is also not to pack, compress, purge or otherwise dispose of files and parts of files unless a true and correct copy of such files is made.

Your client is to preserve and not destroy all passwords, decryption procedures (including, if necessary, the software to decrypt the files); network access codes, ID names, manuals, tutorials, written instructions, decompression or reconstruction software, and any and all other information and things necessary to access, view and (if necessary) reconstruct the electronic data we will request through discovery.

Documents Subject to Preservation Notice:

1. **Business Records:** [All documents and information about documents containing backup and/or archive policy and/or procedure, document retention policy, names of backup and/or archive software, names and addresses of any offsite storage provider.]
 - a. All e-mail and information about e-mail (including message contents, header information and logs of e-mail system usage) (sent or received) by the following persons:
[List names, job titles]
 - b. All other e-mail and information about e-mail (including message contents, header information and logs of e-mail system usage) containing information about or related to:
[Insert detail]
 - c. All databases (including all records and fields and structural information in such databases), containing any reference to and/or information about or related to:
[Insert detail]
 - d. All logs of activity (both in paper and electronic formats) on computer systems and networks that have or may have been used to process or store electronic data containing information about or related to:
[Insert detail]
 - e. All word processing files, including prior drafts, "deleted" files, and file fragments, containing information about or related to:
[Insert detail]
 - f. With regard to electronic data created by application programs that process financial, accounting and billing information, all electronic data files, including prior drafts, "deleted" files, and file fragments, containing information about or related to:
[Insert detail]
 - g. All files, including prior drafts, "deleted" files, and file fragments, containing information from electronic calendars and scheduling programs regarding or related to:
[Insert detail]
 - h. All electronic data files, including prior drafts, "deleted," files and file fragments about or related to:
[Insert detail]
2. **Online Data Storage on Mainframes and Minicomputers:** With regard to online storage and/or direct access storage devices attached to your company's mainframe computers and/or minicomputers: they are not to modify or delete

any electronic data files, "deleted" files and file fragments existing at the time of this letter's delivery, which meet the definitions set forth in this letter, unless a true and correct copy of each such electronic data file has been made and steps have been taken to ensure that such a copy will be preserved and accessible for purposes of this litigation.

3. **Offline Data Storage, Backups and Archives, Floppy Diskettes, Tapes, and Other Removable Electronic Media:** With regard to all electronic media used for offline storage, including magnetic tapes and cartridges and other media that, at the time of this letter's delivery, contained any electronic data meeting the criteria listed in paragraph 1 above: Your client is to stop any activity that may result in the loss of such electronic data, including rotation, destruction, overwriting and/or erasure of such media in whole or in part. This request is intended to cover all removable electronic media used for data storage in connection with their computer systems, including magnetic tapes and cartridges, magneto-optical disks, floppy diskettes, and all other media, whether used with personal computers, minicomputers, or mainframes or other computers, and whether containing backup and/or archive data sets and other electronic data, for all of their computer systems.
4. **Replacement of Data Storage Devices:** Your client is not to dispose of any electronic data storage devices and/or media that may be replaced due to failure and/or upgrade and/or other reasons that may contain electronic data meeting the criteria listed in paragraph 1 above.
5. **Fixed Drives on Stand-Alone Personal Computers and Network Workstations:** With regard to electronic data meeting the criteria listed in paragraph 1 above, which existed on fixed drives attached to stand-alone microcomputers and/or network workstations at the time of this letter's delivery: Your client is not to alter, erase, wipe, or scrub such electronic data, and not to perform other procedures (such as data compression and disk defragmentation or optimization routines) that may impact such data, unless a true and correct copy has been made of such active files and of completely restored versions of such deleted electronic files and file fragments, copies have been made of all directory listings (including hidden files) for all directories and subdirectories containing such files, and arrangements have been made to preserve copies during the pendency of this litigation.
6. **Programs and Utilities:** Your client is to preserve copies of all application programs and utilities, which may be used to process electronic data covered by this letter.
7. **Log of System Modifications:** Your client is to maintain an activity log to document modifications made to any electronic data processing system that may affect the system's capability to process any electronic data meeting the criteria listed in paragraph 1 above, regardless of whether such modifications were made by employees, contractors, vendors and/or any other third parties.
8. **Personal Computers, PDAs, Cell Phones, Voice Mail And Other Devices Used by Employees and/or Their Secretaries and Assistants:** The following

steps should immediately be taken in regard to all personal computers, PDAs, cell phones, voice mail and other devices used by your client's employees and/or their secretaries and assistants.

- a. As to fixed drives attached to such computers: (i) a true and correct copy is to be made of all electronic data on such fixed drives relating to this matter, including all active files and completely restored versions of all deleted electronic files and file fragments; (ii) full directory listings (including hidden files) for all directories and subdirectories (including hidden directories) on such fixed drives should be written; and (iii) such copies and listings are to be preserved until this matter reaches its final resolution.
 - b. All floppy diskettes, magnetic tapes and cartridges, and other media used in connection with such computers prior to the date of delivery of this letter containing any electronic data relating to this matter are to be collected and put into storage for the duration of this lawsuit.
9. **Evidence Created Subsequent to This Letter:** With regard to electronic data created subsequent to the date of delivery of this letter, relevant evidence is not to be destroyed and your client is to take whatever steps are appropriate to avoid destruction of evidence.

To assure that you and your client's obligation to preserve documents and things will be met, please forward a copy of this letter to all persons and entities with custodial responsibility for the items referred to in this letter. We expect that you will monitor compliance.

[Press F11, Type Closing]

Form V

Investigating Expert Witnesses via the Internet

1. Develop a working knowledge of the expertise by reading books and articles. This can also lead you to the experts in the field or help verify credentials for the experts you already have.

Suggested web sites to review:

<http://sunsite.berkeley.edu/Libweb>
<http://catalog.loc.gov/>
<http://www.refdesk.com/>
<http://www.ipl.org/div/aon>

2. Review the expert's writings.

Suggested web sites to review:

<http://www.FindArticles.com>
<http://www.ingentaconnect.com/>

3. Search free expert witness directories.

Suggested web sites to review:

<http://www.jurispro.com/>
<http://www.experts.com/>
<http://www.almexperts.com/ExpertWitness/>
<http://www.expertclick.com/>
<http://expertpages.com/>
http://marketcenter.findlaw.com/expert_witnesses.html
<http://www.witness.net/>
<http://www.idex.com/about/index.html>

4. Find the expert's conference presentations.

Suggested web sites to review:

<http://www.google.com> (Advanced Search – Microsoft PowerPoint)

5. Join an on-line community to find experts' postings or to learn about the topic.

Suggested web sites to review:

<http://www.lsoft.com/lists/listref.html>
<http://lists.topica.com/>
<http://lists.megalink.net/archives/expert-l.html>
<http://groups.google.com/>

6. Review the expert's own Web site.

7. Determine if the expert has ever been disciplined.

Suggested web sites to review:

<http://www.idex.com/about/index.html>

8. Find experts via jury verdict reporter databases.

Suggested web sites to review:

<http://www.morelaw.com/verdicts/>
<http://www.verdictsearch.com/>
<http://www.juryverdicts.com/experts/index.html>

9. Find the expert's deposition testimony.

Suggested web sites to review:

<http://www.trialsmith.com/>
<http://www.dri.org/>

10. Find briefs and cases that refer to the expert.

Suggested web sites to review:

<http://www.briefreports.com/>
<http://www.briefserve.com/home.asp>

11. Locate academic experts through university sites.

Suggested web sites to review:

<http://www.clas.ufl.edu/CLAS/american-universities.html>

12. Find government experts through government reports.

Suggested web sites to review:

<http://www.usa.gov/>

13. Use pay referral sites.

Suggested web sites to review:

<http://www.forensisgroup.com/>
<http://www.tasanet.com/>