MILBERG WEISS

Ariana J. Tadler
Direct Dial: 212-946-9453
atadler@milbergweiss.com

RECEIVED 1/7/05

04-CV-076
Request to Testify
2/11 DC

January 7, 2005

VIA FACSIMILE: 202-502-1766
Mr. Peter G. McCabe
Secretary
Administrative Office of the U.S. Courts
One Columbus Circle, NE
Washington, DC 20544

Re: Request to testify at February 11, 2005 Washington, DC Hearing:
Proposed Amendments regarding e-Discovery

Dear Peter:

As a follow up to your conversation with Sol Schreiber of my firm, I respectfully request an opportunity to be heard at the February 11, 2005 Washington, DC Hearing regarding the Proposed Amendments regarding e-Discovery.

Should you have any questions, please do not hesitate to contact me.

Sincerely,

Ariana J. Tadler

AJT:lar

04-CV-076
Testimony
2/11 DC

MILBERG WEISS

Ariana J. Tadler
Direct Dial: 212-946-9453
atadler@milbergweiss.com

February 4, 2005

VIA E-MAIL AND FACSIMILE

Peter G. McCabe, Secretary
Committee on Rules of Practice and Procedure
Administrative Office of the United States Courts
Washington, DC 20544

Re: *Proposed Federal Civil Rule Amendments: Electronic Discovery*

Dear Peter:

I write to address briefly some of my views concerning the proposed amendments to the Federal Civil Rules governing electronic discovery in advance of my anticipated testimony on or about February 12, 2005. My comments are based upon my personal experiences as a litigator (including, most recently, my role in the *Initial Public Offering Securities Litigation*, *see infra*), daily interaction and discussions with my partners and the firm's associates regarding their personal experiences, my direct supervision of the firm's Director of Litigation Technology Support and my continuing and active interest in, and frequent participation on, panels nationwide regarding the topic of electronic discovery.

SUMMARY

As discussed more fully below, my and my colleagues' experiences lead me to (i) ***applaud*** the proposed amendments to the extent they *identify* electronic discovery/information as that which should be considered (although not necessarily pursued) by parties and judges at an early stage, depending on the circumstances of particular litigation (*e.g.*, Proposed Amendments 16(b)(5), 26(f), 33), but (ii) ***strongly oppose*** any proposal which inevitably will erect additional hurdles or obstacles to the fact-finding process and create further imbalance on the litigation "playing field" in favor of the responding party and to the detriment of the party who bears the burden of proof, such as the establishment of standards limiting the scope of production based upon purported "inaccessibility" (Proposed Amendment 26(b)(2)) or a "safe harbor" for evidence destruction (Proposed Amendment 37(f)), *i.e.* destruction of information which is uniquely in the possession of the party against whom a claim has been or is likely to be asserted.

Significant changes in the existing law, such as those contemplated by most, if not all of the remaining proposed amendments, should be approached cautiously. Given (i) the still nascent stage of any real understanding of the problems (and appropriate solutions) encountered by "electronic discovery" (as distinguished from electronic information), (ii) the evolving but still limited case law addressing many novel but critical issues (only a handful of judges have published detailed opinions on the subject), and (iii) a fairly large, still uninformed practitioner population as to the significance of these issues, substantive amendments governing electronic discovery are, I respectfully submit, premature and unwarranted at this stage. Any rules governing discovery must be sufficiently flexible to accommodate the continuous evolution of information management and development and, more importantly, fair and reasonable to allow discovery of the truth. In many respects, the current procedural regime already provides the necessary flexibility and fairness, when properly utilized and applied.

BACKGROUND

I am a member of Milberg Weiss Bershad & Schulman LLP, a national law firm of more than 120 lawyers with principal offices in New York City and additional offices in Boca Raton, Florida; Wilmington, Delaware; Washington, D.C.; Seattle, Washington; and Los Angeles, California. Over the past forty years, the firm's practice has focused on the prosecution of class and complex actions in many fields of commercial litigation, emphasizing securities, corporate fiduciary, consumer, insurance, healthcare, antitrust, mass tort, human rights, and related areas of litigation.

The firm is particularly well-known for its role in litigating and managing particularly large, high-profile class actions against some of the largest companies and involving some of the biggest industries in the world. These lawsuits inevitably involve intense and voluminous discovery leading to the production and review of millions of "pages"/ "images" of information. Among such cases is the *Initial Public Offering Securities Litigation*, 21 MC 92 (SAS) ("*IPO Litigation*"), pending in the United States District Court for the Southern District of New York, in which my senior partner Melvyn Weiss serves as Chairman of the Plaintiffs' Counsel's Executive Committee, and I serve as an appointed liaison to the Court. In that capacity, I manage, on a day-to-day basis, 309 separate class actions which have been coordinated for pretrial purposes. Among the thousands of defendants in these actions are 55 of this nation's most prominent investment banks and more than 300 corporate issuers, many of which are in the high tech industry, and all of which conduct their daily businesses dependent on the use of technology (including, *e.g.*, email, myriad databases, trading systems, internal proprietary programs, etc.). To date, approximately 20 million "pages" of documents have been produced in this litigation, and discovery is ongoing.

Needless to say, electronic discovery has been the leading subject of the parties' discovery negotiations throughout the course of the *IPO Litigation*. Indeed, when the litigation first commenced, only a select few of the hundreds of lawyers in the cases were well-versed, or even somewhat educated, in "e-discovery" terminology or the myriad attendant issues relating to preservation and production of electronic information. Mind you, many of the law firms involved in this litigation are among the most sophisticated and well-known in the country

representing national corporate giants. However, even their lawyers were not well-informed about the relevant issues just two years ago.

DISCUSSION

In truth, many lawyers who practice in federal court, and who seek guidance from the Federal Rules of Civil Procedure and the corresponding Advisory Committee Notes, are similarly uninformed as to these emerging issues. Moreover, many of them do *not* work for big, well-resourced law firms which are more likely to be exposed to such issues. Rather, many of them work for small firms or are sole practitioners representing small entities or individual clients who themselves may not rely on technology in their daily lives or businesses and thus may not otherwise be focused on the fact that their adversaries may very well have electronic information relevant to their claims or potential defenses.[1]

These facts and my most recent experiences in the *IPO Litigation* (as well as reported experiences of my colleagues) lead me to applaud the proposed amendments to the rules which ***force*** otherwise techno-ignorant or, perhaps worse, techno-phobic, lawyers (and judges) to educate themselves about and pursue or at least consider the need for electronic discovery (*e.g.*, Proposed Amendments 16(b)(5), 26(f) (including 26(f)(3) highlighting the need to consider and address preservation and the forms of production of electronic information at an early stage of the case), 33 and 45(a)). This educational element of the proposed amendments is critical given the era in which we live – an era in which, at least as of today, technology like email, instant messaging, RightFax or e-Fax, and electronic databases serve as principal means of communication, negotiation and information management, making, in many instances (businesses and individuals alike), traditional paper correspondence and other paper documentation obsolete. Highlighting this form of information in the actual wording of the Rules helps to educate (or, at least, serve as a reminder to) lawyers who, in the past, may not have considered or pursued electronic information/discovery and who, even today, may not use such forms of technology in their ordinary course of business. It is extremely wise to focus on this critical means of communication and information storage which, in today's reality, is more likely to be the evidentiary treasure trove that paper files once were. Indeed, electronic information can be a critical source of evidence of elements like scienter and thus must be carefully considered. In addition, motivating lawyers to meet and confer and/or to consider and identify the requested form of production is a practical, and traditionally successful, solution to reducing litigation costs, including motion practice.

---

[1] My father is a prime example. He is a sole practitioner who until very recently rarely used email himself. Until recently, he and his adversaries rarely considered electronic information as a source of discovery. However, with the actual identification of these issues in the proposed amendments (and some prodding from his insistent daughter), he now recognizes that electronic information should not be simply overlooked but rather considered and, *where appropriate and within reason*, pursued.

In contrast to the proposed and much needed *identification* of electronic discovery in the proposed amendments as among the forms of information to be considered and potentially pursued in the course of discovery, and the prompting of thought and discussion about issues like preservation and forms of production, the additional proposed amendments are, for the most part, unduly conservative and inequitable and likely to lead to further discovery abuse and motion practice. (*See, e.g.*, Proposed Amendments 26(b)(2), 26(b)(5), 37(f), 45(d)(1)(C), 45(d)(2)(B)).

To address concerns regarding scope, burden, costs and fairness, parties and their counsel should be encouraged by the Advisory Committee Notes to maximize their use of the traditional meet and confer process and utilize (i) formal discovery mechanisms currently in existence (*e.g.*, 30(b)(6) depositions and interrogatories), as well as (ii) informal, creative devices such as questionnaires or interviews, to educate themselves about the types of information available from the parties in each case, the form(s) in which that information is maintained and/or utilized, how one can access such forms of information, the potential burden to compile and produce such information, the costs associated with accessing and producing such information and to assess whether court intervention is necessary. Proper use of these historically underutilized tools at an early stage in litigation (*e.g.*, before or immediately after service of discovery requests), *rather than the rigid standards and presumptions contemplated by the amendments which risk the establishment of even greater hurdles to the fact-finding process*, will encourage lawyers and judges to assess the facts and circumstances of *each case* and will guide decisions regarding the appropriate scope, burden and costs to be incurred in *each particular case*. Indeed, if practitioners and judges have learned anything about discovery, including, in particular, electronic discovery, it is that one size does *not* fit all.

For example, in the *IPO Litigation*, the parties, adequately left to their own devices in the absence of strict guidance from the Rules, were forced to be creative and responsibly work together to establish a series of tools to assist in educating themselves as to the relevant forms and volumes of information in the possession of each of the parties *and* to negotiate a series of terms and parameters to govern the preservation and production of electronic discovery in this mammoth litigation which were ultimately presented to and approved by the Court. Indeed, notwithstanding the information preservation provisions of the Private Securities Litigation Reform Act, 15 U.S.C. §78u-4(b)(2), the parties acted practically, recognizing that the preservation of *all* forms of potentially relevant information for the duration of the litigation would not be reasonable given the ongoing businesses of the parties, and negotiated a detailed Document Preservation Protocol which the Court approved and entered as an order. A copy of that protocol is attached hereto as Exhibit A.

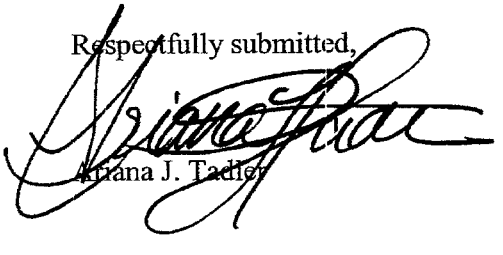
The protocol sets forth basic provisions governing, among other things, the recycling of backup tapes, the maintenance of legacy software and hardware to ensure access to information, and the preservation/copying of potentially relevant hard drives. These provisions were negotiated after a series of discussions among the parties regarding their respective internal systems and the maintenance of information and based upon answers to a series of detailed questions regarding the parties' document retention practices and procedures. (The questionnaire is Schedule C to the Document Preservation Protocol). Questionnaires and preservation protocols like those utilized in the *IPO Litigation* can serve as helpful tools in paring down the

scope of discovery in an equitable fashion, based on real, verifiable facts, so as to address fairly the opposing concerns of competing parties (*e.g.*, preservation of potentially relevant information v. the volume of production and purported burden and associated costs). In stark contrast, the proposed establishment of a standard permitting a party to refuse to produce based on purported "inaccessibility" or a safe harbor without adequate and reliable safeguards may well lead to significant mischief (far beyond that which we have seen in the past). For example, Proposed Amendment 26(b)(2) provides the responding party with an incentive to (i) stall, with the burden then shifting to the requesting party to pursue motion practice based on facts uniquely in the possession of the responding party, or worse, (ii) routinely transfer data to media which appear to be "not reasonably accessible" for purposes of litigation but in reality remain (or, with the rapid evolution of technology, may become) readily accessible for business purposes by the simple touch of a keyboard button or the execution of a simple program. Such incentives belie the very premise of our procedural system for which the Rules *must* provide support -- the search for and discovery of the truth.

CONCLUSION

In sum, I strongly advocate that the Committee (i) consider the comments of all submitting parties with an open mind and an eye towards maintaining a level playing field in the courtroom; (ii) focus on the *substance* of the comments to ensure consistent and equitable means for the pursuit of the truth through discovery rather than the sheer volume of comments received from any particular lawyer/client contingency or interest group; (iii) recognize that the sheer volume of comments on behalf of corporate lawyers, representative associations and their clients should not itself persuade the Committee that the proposed amendments are appropriate or fair; and (iv) recognize that many lawyers and client citizens continue to remain uneducated and uninformed regarding the issues relevant, indeed critical, to an evaluation of the fairness of the proposed amendments such that any decisions/proposals at this time, at least insofar as they propose significant changes/presumptions, are premature and would create a serious risk of deleterious and inequitable results. Thus, continued solicitation of comments regarding proposed rules governing electronic discovery (including reports of practical experiences and applied solutions) from a wide variety of judges and practitioners is strongly warranted and urged.

Respectfully submitted,



Ariana J. Tadler

AJT:lr
Attachment

EXHIBIT A

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In re **INITIAL PUBLIC OFFERING SECURITIES LITIGATION** This Document Relates to All Cases	21 MC 92 (SAS) **PROPOSED CASE MANAGEMENT ORDER RELATING TO PRESERVATION OF ELECTRONIC DATA**

SHIRA A. SCHEINDLIN, U.S.D.J.:

Annexed hereto as Exhibit 1 is a Protocol for the Preservation of Electronic Data ("Protocol") that has been submitted by the parties listed in Schedules A and B thereto. IT IS HEREBY ORDERED that the parties identified in Schedules A and B to the Protocol abide by the provisions thereof.

Shira A. Scheindlin, U.S.D.J.

Dated: December 19, 2002
New York, New York

EXHIBIT 1

Plaintiffs' and Underwriter Defendants' Joint Proposed Electronic Data Preservation Protocol

1. As used herein, the term "potentially discoverable electronic information" refers to Underwriter Defendants' and Institutional Named Plaintiffs' electronic "documents" that contain or potentially contain information relating to facts at issue in the litigation, where the term "documents" is used as it is defined in Fed. R. Civ. P. 34(a).[1]

2. During the pendency of these actions, the Underwriter Defendants and the Institutional Named Plaintiffs shall securely maintain, to the extent that they currently exist and may contain potentially discoverable electronic information: (i) e-mail back-up tapes, and (ii) network back-up tapes (together, the "Back-Up Tapes") created in the ordinary course of business during the period from August 1997 through August 2002 as set forth in the following sentence. The Underwriter Defendants and the Institutional Named Plaintiffs shall be obligated to retain only one day's Back-Up Tapes among all Back-Up Tapes created in the ordinary course during a given month, provided that such day's Back-Up Tapes represent a complete back-up of the data contained on the subject servers on that day (as opposed to merely an incremental back-up of the subject servers). If only incremental back-up tapes have been retained for a given month, then all such incremental tapes shall be retained. All Back-Up Tapes other than those specifically required to be preserved pursuant to this paragraph and paragraph 3 below may be recycled, overwritten, or erased, as the case may be, pursuant to each Underwriter Defendant's and Institutional Named Plaintiff's otherwise applicable retention schedule.

3. All electronic information or data archived or backed up during the period from August 1997 through August 2002 as part of a special back-up (a back-up made other than in the ordinary course of business by an Underwriter Defendant or Institutional Named Plaintiff), whether due to system upgrade, transition planning, system migration, disaster recovery planning, Y2K testing, or any other reason, that potentially contains potentially discoverable electronic information shall be securely retained, to the extent that they currently exist, for the remainder of the litigation.

4. All current or legacy software and hardware necessary to access, manipulate, print, etc., potentially discoverable electronic information that either is "live" or has been archived or backed up shall be securely retained, to the extent that they currently exist, for the remainder of the litigation.

---

[1] The Underwriter Defendants consenting to this protocol are set forth in Schedule A, annexed hereto. The agreed-upon Institutional Named Plaintiffs subject to this protocol are set forth in Schedule B, annexed hereto.

5. The Underwriter Defendants and the Institutional Named Plaintiffs shall circulate retention notices designed to ensure the preservation of potentially discoverable electronic and other information to those employees potentially possessing such information. Thereafter, the Underwriter Defendants and the Institutional Named Plaintiffs shall quarterly re-notify their employees of their continuing obligation to preserve such information.

6. The Underwriter Defendants and the Institutional Named Plaintiffs shall take the following measures to secure and retain, to the extent that it exists, the potentially discoverable electronic information that is on the desktop and laptop hard drives of their respective employees. Either: (i) hard drives containing potentially discoverable electronic data shall be retained with all potentially discoverable electronic data contained therein retained intact; or, (ii) employees shall be instructed to copy all potentially discoverable electronic information to a secure, backed-up network storage device or back-up medium for the remainder of the litigation, making all reasonable efforts to retain all meta-data (file creation dates, modification dates, etc.) associated with the potentially discoverable electronic information at issue. The periodic retention notifications disseminated pursuant to paragraph 5 above shall advise employees potentially possessing potentially discoverable electronic information of their obligation to store discoverable electronic information on a secure, backed-up network storage device or back-up medium to ensure its preservation and instruct such employees in the manner of doing so in accordance with this paragraph.

7. Plaintiffs within 15 days of receiving the list of business units referred to below shall identify by name, title, or departmental category employees of each Underwriter Defendant for which the respective Underwriter Defendant shall be responsible for maintaining the hard drive, or a mirror image copy (*i.e.*, a bit by bit copy) of such hard drive, during the pendency of this litigation. Defendants shall within 15 days of receiving the list of business units referred to below identify by name, title, or departmental category of employees of Institutional Named Plaintiffs for which the respective Plaintiff shall be responsible for maintaining the hard drive, or a mirror image copy (*i.e.*, a bit by bit copy) of such hard drive, during the pendency of this litigation. In no event shall the number of computers subject to the provisions of this paragraph be greater than 40 for each Underwriter Defendant and 5 for each Institutional Named Plaintiff. The hard drives or image copies of such hard drives preserved pursuant to this paragraph shall be labeled to identify the employee who primarily used the computer associated with that hard drive. In order to facilitate the identification of the appropriate employees, the parties will provide to each other identification by business unit and positions the employees they reasonably believe could have potentially discoverable electronic information. The parties will meet and confer in good faith and exchange additional information as may be necessary to facilitate the identification, and limit the number, of employees for whom the provisions of this paragraph shall be applicable.

8. To the extent that any Underwriter Defendant or Institutional Named Plaintiff has implemented a system for the purpose of preserving external emails (emails sent to or received by a given Underwriter Defendant's or Institutional Named Plaintiff's employees) in an easily accessible form, other than an email server or the Back-up Tapes

identified in paragraph 2 or 3 above, all emails that were created during the period from August 1997 through August 2002, that contain potentially discoverable electronic information, and that are stored on any such system as of the date hereof, shall be preserved during the pendency of this litigation.

9. Within 45 days, each Underwriter Defendant and each Institutional Named Plaintiff will provide written answers to the best of its ability to the questions concerning information system and electronic document retention practices set forth in attached Schedule C. Should any Underwriter Defendant or Institutional Named Plaintiff believe that it cannot in good faith answer any of the questions as posed, the relevant parties will confer to resolve any disputes and, if necessary, seek Court intervention.

10. By agreeing to preserve potentially discoverable electronic information in accordance with the terms hereof, none of the Underwriter Defendants and none of the Institutional Named Plaintiffs are waiving any objection to the ultimate discoverability of such information at such point when discovery is authorized in these actions.

11. Nothing herein shall be deemed to affect the Underwriter Defendants' and Institutional Named Plaintiffs' obligations to preserve hardcopy documents pursuant to paragraph V of the Court's August 8, 2001 Order. If counsel to an Underwriter Defendant or an Institutional Named Plaintiff learns that potentially discoverable hardcopy documents pertaining to a given public offering were destroyed by such party subsequent to being named as a party in, and receiving a copy of, a complaint pertaining to that public offering, counsel for such party shall notify opposing counsel in writing of such destruction within two weeks of learning so.

12. Nothing herein shall preclude any party from raising with counsel or the Court the limitation or modification of the foregoing in response to particular facts relevant to that party.

13. Nothing herein relieves any other party of its obligations under the Federal Rules of Civil Procedure, the Private Securities Litigation Reform Act, or any other applicable law.

SCHEDULE A

Underwriter Defendants Consenting to Plaintiffs' and Underwriter Defendants' Joint Proposed Electronic Data Preservation Protocol

1. Banc of America Securities, LLC (f/k/a NationsBanc Montgomery Securities)
2. The Bear Stearns Companies Inc. and Bear, Stearns & Co. Inc.
3. CIBC World Markets Corp. (f/k/a CIBC Oppenheimer Corp.)
4. Credit Suisse First Boston Corp.
5. Dain Rauscher Wessels (acquired by Royal Bank of Canada in September 2000 and renamed RBC Dain Rauscher, Inc.)
6. Deutsche Bank Securities Inc. (f/k/a Deutsche Bank Alex. Brown and BT Alex. Brown)
7. Epoch Partners (acquired by The Goldman Sachs Group, Inc. in June 2001)
8. E*Offering Corporation (merged into Wit SoundView Corporation, a susidiary of Wit SoundView Group, Inc., in October 2000; subsequently known as SoundView Technology Corporation)
9. Everen Securities Holdings, Inc. (a subsidiary of Everen Captial Corporation, acquired by First Union Corporation in April 1999)
10. The Goldman Sachs Group, Inc. and Goldman, Sachs & Co.
11. J.C. Bradford & Co. (acquired by Paine Webber Group, Inc. in April 2000)
12. J.P. Morgan Securities Inc. (Hambrecht & Quist, LLC, Chase Securities, Inc., and J.P. Morgan Securities merged into a single entity)
13. Lazard Freres & Co., LLC
14. Lehman Brothers Holdings, Inc. and Lehman Brothers, Inc.
15. Merrill Lynch & Co., Inc., Merrill Lynch, Pierce, Fenner & Smith Incorporated and Merrill Lynch International
16. Morgan Stanley Dean Witter & Co., Morgan Stanley & Co. and Morgan Stanley Online
17. Needham & Company, Inc.
18. Paine Webber Group, Inc. (acquired by UBS Warburg, LLC in November 2000 to form UBS Paine Webber, Inc.)
19. Prudential Securities Incorporated (individually and as successor in interest to Volpe Brown Whelan & Co., LLC)

20. Raymond James & Associates
21. Robert Fleming Inc. (acquired by Chase H&Q in August 1999)
22. Robertson Stephens, Inc. (f/k/a BancBoston Robertson Stephens, Inc. and FleetBoston Robertson Stephens, Inc.)
23. Salomon Smith Barney, Inc.
24. SG Cowen Securities Corp.
25. SoundView Technology Group, Inc. (a wholly owned subsidiary of Wit Capital Group, Inc. as of January 2000; subsequently known as Wit SoundView Corporation and SoundView Technology Corporation)
26. SunTrust Robinson Humphrey Capital Markets a division of SunTrust Capital Markets, Inc.
27. Thomas Weisel Partners, LLC
28. Tucker Anthony Inc. (acquired by the parent of RBC Dain Rauscher Inc. in November 2001 and merged into RBC Dain Rauscher Inc. in March 2002)
29. UBS Paine Webber, Inc. (formed by November 2000 acquisition of Paine Webber Group, Inc. by USB Warburg, LLC)
30. UBS Warburg, LLC (formed by June 1998 merger of SBC Warburg and Union Bank of Switzerland)
31. U.S. Bancorp Piper Jaffray, Inc.
32. Wit Capital Group, Inc. (subsequently known as Wit SoundView Group Inc., and SoundView Technology Group, Inc.)
33. Wit SoundView Group Inc. (formerly known as Wit Capital Group, Inc.)

SCHEDULE B

Institutional Plaintiffs

Issuer	Docket Number	Plaintiff
Avanex	01 Civ. 6890	International Brotherhood of Electrical Workers
eBenX, Inc.	01 Civ. 9411	Rennel Trading Corp.
eGain Comm., Corp.	01 Civ. 9414	Rennel Trading Corp.
Eloquent, Inc.	01 Civ. 6775	Pond Equities
GRIC Communications, Inc.	01 Civ. 6771	Colbert Birnet, LP
InforMax, Inc.	01 Civ. 10834	Coastline Corporation, Inc.
Internet Capital Group, Inc.	01 Civ. 3975	AFA Management Partners, LP
Metasolv Software, Inc.	01 Civ. 9651	Colbert Birnet, L.P.
Numerical Technologies	01 Civ. 9513	Pond Equities
On Semiconductor Corp.	01 Civ. 6114	Fuller & Thaler Asset Management
Palm, Inc.	01 Civ. 5613	Plumbers and Pipefitters National Pension Fund
Perot Systems Corp.	01 Civ. 6820	Robinson Radiology Ltd. Profit Sharing Plan and Trust
Radio One, Inc.	01 Civ. 10160	Colbert Birnet, L.P.
Wireless Facilities, Inc.	01 Civ. 4779	Fuller & Thaler Asset Management

SCHEDULE C

Plaintiffs' and Underwriter Defendants' Proposed Document Retention Questionnaire

Network Servers

The below questions concern the current and former database and file servers on your network that now store or previously stored discoverable electronic data (hereinafter referred to as "network servers").

1. Do you have at least one complete (i.e., non-incremental) backup of each of your network servers for each month since August 1, 1997 to the present?

   1.1. If not, for which months do you not have at least one complete backup?

   1.2. For those months, if any, for which you do not have a complete backup, do you have incremental backups or other backups from which a full backup can be created of all data as of a given date in each such month?

   1.3. If so, please describe the nature of such incremental or other backups and identify the months for which you have them.

2. Can specific files contained on network backups be selectively restored?

3. As a matter of firm policy, do you overwrite, reformat, erase, or otherwise destroy the content of the backups of your network servers on a periodic basis?

   3.1. If so, what is the rotation period?

   3.2. If the rotation period has changed since August 1, 1997, describe the changes.

Email Servers

The below questions concern the current or former servers on your network ("email servers") that now or previously stored discoverable electronic internal or external peer-to-peer messages, including email, Bloomberg email, other third party email sources, and instant messages (collectively, "email").

4. Identify the systems (client and server-side applications) used for email and the time period for the use of each such system.

5. Are end-user emails that appear in any of the following folders stored on (i) the end-user's harddrive, (ii) an email server, or (iii) a server of a third party application service provider:

- "In Box"?
- "Sent Mail"?
- "Delete" or "trash" folder?
- End user stored mail folders?

6. If any of your emails systems have changed since August 1, 1997, identify the legacy system, the new system, and the date of the last backup made with the legacy system.

7. Do you have at least one complete (i.e., non-incremental) back up of each of your email servers for each month since August 1, 1997 to the present?

   7.1. If not, for which months do you not have at least one complete backup?

   7.2. For those months, if any, for which you do not have a complete backup, do you have incremental or other backups from which a full backup can be created of all data as of a given date in each such month?

   7.3. If so, please describe the nature of such incremental or other backups and identify the months for which you have them.

8. Does each complete email backup contain all messages sent or received since creation of the immediately prior complete email backup?

   8.1. Do your email backups contain the messages that are in each employee's "in box" as of the time such backup is made?

   8.2. Do your email backups contain the messages that are in each employee's "sent mail" folder as of the time such backup is made?

   8.3. Do your email backups contain the messages that are in each employee's "delete" or "trash" folder as of the time such backup is made?

   8.4. Do your email backups contain the messages that are in each employee's stored mail folders as of the time such backup is made?

9. Can specific email boxes contained on email backups be restored selectively?

10. As a matter of firm policy, do you overwrite, reformat, erase, or otherwise destroy the content of the backups of your email servers on a periodic basis?

    10.1. If so, what is the rotation period?

    10.2. If the rotation period has changed since August 1, 1997, describe the changes.

11. Do you have a computer system that maintains electronic copies of all emails sent or received by certain of your employees?

    11.1. If so, describe the system(s) and the date(s) of first use.

    11.2. If so, does such system(s) contain copies of all emails captured from the date of first use until the present?

    11.3. If so, does such system(s) capture a copy of all emails sent or received by employees in investment banking, equity research functions, or senior management?

Hard Drives

The below questions concern the current and former local or non-network drives contained in current or former employees' laptop and desktop computers or workstations.

12. As a matter of firm policy, are employees' desktop and laptop hard drives backed up in any way?

    12.1. If so, under what circumstances?

    12.2. If so, how long are such backups retained?

13. As a matter of firm policy, are employees permitted to save files, emails or other data (excluding system and application generated temporary files) to their desktop or laptop hard drives?

14. Since August 1, 1997, has it been technically possible for firm employees to save files, emails, or other data (excluding system and application generated temporary files) to their desktop or laptop hard drives?

15. Do you implement technical impediments to minimize the opportunity for employees to save files, emails or other data (excluding system and application generated temporary files) to their desktop or laptop hard drives?

16. As a matter of firm policy, are employees' desktop and laptop hard drives erased, "wiped," "scrubbed" or reformatted before such hard drives are, for whatever reason, abandoned, transferred or decommissioned?

    16.1. If so, are, as a matter of firm policy, files, emails or other data stored on such hard drives copied to the respective employee's replacement drive, if any?

    16.2. If so, are, as a matter of firm policy, such files, emails or other data copied on a "bit-by-bit" basis?

Non-Firm Computers

17. Does firm policy permit, prohibit or otherwise address employee use of computers not owned or controlled by the firm to create, receive, store or send work-related documents or communications?

    17.1. If so, what is that policy?

18. Is there any technical impediment to employees using computers not owned or controlled by the firm to create, receive, store or send work-related documents or communications?