

A

FOOTE, MEYERS, MIELKE & FLOWERS, LLC

ATTORNEYS AT LAW

PHONE (630) 232-6333  
FACSIMILE (630) 845-8982  
www.foote-meyers.com

28 NORTH FIRST STREET  
SUITE 2  
GENEVA, ILLINOIS 60134

CHICAGO OFFICE  
30 NORTH LASALLE STREET  
SUITE 2340  
CHICAGO, ILLINOIS 60603  
(312) 214-1017

July 2, 2007

Adam L. Barea - Litigation Counsel  
Google Inc.  
1600 Amphitheatre Parkway  
Mountain View, CA 94043

*Re: Vulcan Golf, LLC, v. Google, Inc., Overseer.net, Sedo.com, Dotster, Inc.,  
AKA Revenuedirect.com, Internet Reit, Inc. d/b/a Ireit, Inc., and John  
Does I – X, 07-CV-3371  
Rule 26 Obligations/Request for Preservation of Relevant Information*

Dear Counsel:

I am in receipt of your e-mail requesting an extension of time to answer or otherwise plead in the above-referenced matter. Please be advised that we are agreeable to a thirty (30) day extension, until July 31, 2007. In drafting your Motion for Extension of Time, please advise the Court of our agreement in this regard.

Additionally, this letter is intended to address the Parties' obligations under Rules 16 and 26, and to further serve as Plaintiff's formal demand for the preservation of all documents, data, information, and/or other material (electronic and non-electronic) relevant to the claims set forth in Plaintiff's Complaint, pursuant to the applicable federal discovery rules.

As part of the Rule 26(a) disclosures and other discovery in this case, Plaintiff expects to receive all data and documentation necessary and relevant to the claims alleged in Plaintiff's Complaint, including both electronically and non-electronically maintained data and information.

**A. OBLIGATIONS UNDER RULE 26:**

As you know, Rule 26(a)(1) now includes a category of discoverable material referred to as "electronically stored information." (hereinafter "ESI"). Rule 26(b)(2)(B) sets forth various duties and a two-tiered methodology for addressing requests for electronic discovery. A responding party must:

FOOTE, MEYERS, MIELKE & FLOWERS, LLC

- (1) Identify information available from accessible sources;
- (2) Determine whether information from accessible sources will satisfy the discovery request;
- (3) Determine whether any “harder to access” sources should be searched;
- (4) Identify the nature and content of any source claimed to be “inaccessible”; and,
- (5) Provide a cost estimate related to retrieving and reviewing electronic information that is inaccessible to the responding party.

Rule 26(f) requires that parties promptly address the issue of information sources, inaccessible data, and the burden and cost of obtaining information from inaccessible sources that might contain discoverable material. The rule also provides that the discovering party may request the format in which it wishes to receive electronic information. Pursuant to Rule 26(f), please be advised with respect to Plaintiff that:

**i. Plaintiff Sources of Electronic Information:**

Plaintiff will cooperate with Defendants in producing any and all discoverable electronic information in the format designated by Defendants, native format, or an agreeable and suitable format that is usable by Defendants. Please provide Plaintiff with written confirmation of the preferred electronic format, at your earliest convenience

**ii. Plaintiff Requested Format for Information Received**

Plaintiff believes that Defendant is in possession of ESI relevant to the claims asserted in the Complaint. Plaintiff requests that all such information be supplied in either:

- (1) “native format” with all metadata, or
- (2) Another format that retains all metadata and is searchable

If neither of the above is available, Plaintiff requests that Defendant contact Plaintiff to agree upon a suitable form that is reasonably usable and includes all metadata. Further, if the native format of the data is awkward, difficult to produce, or would make it difficult to work with the information, Defendant is requested to confer with Plaintiff to agree upon conversion to another more usable format.

**iii. Defendant Identification of ESI**

FOOTE, MEYERS, MIELKE & FLOWERS, LLC

With respect to Defendant, Plaintiff hereby demands that pursuant to Rule 26(f), Defendant immediately identify each and every potential electronic source of information relevant to claims alleged in the complaint, and the specific format in which such information is maintained. Please also identify any electronic sources that you allege are inaccessible, the data contained in the alleged inaccessible source, and the cost/burden of accessing said information. In meeting your obligations to identify data sources and formats, please include, but do not limit, your Rule 26(f) response to the following:

- Data sources in use, including PDAs, laptop computers, home offices, desktop computers, cell phones, e-mail, flash drives and any other electronic device used by Defendant capable of retaining information
- The operating systems, applications, and databases the company uses and has previously used, dates of use, and access to discontinued software; and
- All hardware and software used by Defendant during the relevant time frame set forth in the Complaint and the relevant dates of use.

**iv. Rule 26 (f) Conference**

Due to the nature of the claims in Plaintiff's Complaint, electronically stored information will undoubtedly comprise a large portion of discovery. Rule 26(a) requires that parties, without awaiting a discovery request, promptly identify and produce ESI, documents and tangible things in a party's possession, custody and control that the party may use to support its claims or defenses. *F.R.C.P. Rule 26(a)(1)* Further, Rule 26(f) mandates that the parties confer "to discuss any issues relating to preserving discoverable information" prior to the Rule 16 Scheduling Conference. *F.R.C.P. Rule 26(f)*. Further, it is our intention to seek inclusion in the Court's Rule 16 scheduling order "provisions for disclosure or discovery of electronically stored information" and "any agreements the parties reach for asserting claims of privilege or of protection as trial-preparation material after production." Rules 16(b)(5) and (b)(6). Therefore, it is critically important that at the earliest possible date, we arrange to "meet and confer," pursuant to our obligations

**FOOTE, MEYERS, MIELKE & FLOWERS, LLC**

under both Rules 16 and 26. Please be advised that we intend for the Parties, at our Rule 26(f) conference, to among other things :

1. **Identify the nature and extent of potentially relevant electronic evidence.**
2. **Discuss preservation of ESI and tangible documents/evidence and steps required to prevent spoliation.**
3. **Define production scope (e.g., which types of evidence, what computer systems/databases, and geographic locations.**
4. **Discuss and outline scope/timeframe/searching strategies/priority of production of ESI.**
5. **Identify potential problems or special handling requirements that could impact production.**
6. **Discuss and establish production protocol, such as formatting, labeling, and tracking issues to minimize production delays and confusion stemming from problems that typically arise during the course of electronic production.**
7. **Discuss and establish production dispute resolution procedures.**
8. **Discuss and establish key production timeline and milestones.**
9. **Identify what policies and practices govern the retention of electronic records.**
10. **Identify those computers where there is uncertainty as to whether or not they contain relevant electronic evidence, including, but not limited to:**
  - a. Type of system
  - b. What is the means for determining whether or not they contain evidence?
  - c. How soon can the determination be made?
11. **Discuss policies that govern upgrades/disposal/redeployment of computer hardware such as servers/desktop/laptop systems.**
12. **For each system that is believed to contain relevant evidence, discuss and determine how far back does "live" data go.**

FOOTE, MEYERS, MIELKE & FLOWERS, LLC

13. Determine and identify whether there are any imminent software upgrades or conversions imminent which might render certain types of data less accessible.
14. For each system believe to contain relevant evidence, determine and identify what type of backups/archival copies may exist.
15. Determine and identify the key applications of database systems that contain or likely contain relevant evidence, for example:
  - a. E-Mail?
  - b. Office Documents?
  - c. Custom Applications?
  - d. Databases?
  - e. Demographic and statistical analysis systems?
  - f. Computer access logs?
16. For each key system, determine and identify the primary software used to support the system, for example:
  - a. **In regard to E-mail (Lotus Notes, Outlook, other):**
    - i. What software is used for e-mail server and e-mail client?
    - ii. Has a strategy been identified to search/preserve e-mails?
    - iii. How many e-mail servers are to be searched?
    - iv. Can the strategy be applied to all e-mail or only what is on the mail server now?
    - v. What would be required to search mail saved by users to personal folders?
    - vi. Will individual user computers and servers be searched?
    - vii. What would be required to search all mail backups?
    - viii. If users are conducting their own searches, will their process and compliance be identified and verified?
  - b. **In regard to Office Documents**
    - i. Applicable dates of use;
    - ii. Versions used;
    - iii. What strategy will be used for searching/extracting relevant records?
    - iv. What is the proposed production format?
    - v. What media (disk/tape/DVD) will be used for the production?
    - vi. How much data is likely to be produced (in units of records, megabytes, or other unit that will give a sense of the overall volume)?
  - c. **In regard to Custom Applications:**
    - i. What business purpose did the software provide?

FOOTE, MEYERS, MIELKE & FLOWERS, LLC

- ii. Date of use?
- iii. Creator(s)
- iv. What types of data storage (flat file, database, EDI, proprietary, etc.) were used?
- v. What record formats/fields were used in this data?
- vi. Is information about encoding/abbreviations used within data available to make sense of the data?
- vii. What strategy will be used for searching/extracting relevant records?
- viii. What is the proposed production format?
- ix. What media (disk/tape/DVD) will be used for the production?
- x. How much data is likely to be produced (in units of records, megabytes, or other unit that will give a sense of the overall volume)?

**d. In regard to Key Database:**

- i. What types of databases (Oracle, DB2, IMS, etc.) were used and what version numbers?
- ii. What is the primary business purpose(s)?
- iii. What type of data does it contain? (Detail, summary, statistical, cumulative or point-in-time?)
- iv. Is information available that defines table/row format and relationships needed to determine production/redaction requirements?
- v. Is documentation available to define encoding and abbreviations used within the data?
- vi. What strategy will be used for searching/extracting relevant records?
- vii. What is the proposed production format?
- viii. What media (disk/tape/DVD) will be used for the production?
- ix. How much data is likely that will give a sense of the overall volume)?

**17. Determine and identify how many computer systems are known to contain relevant evidence, for example:**

- a. Type of system (e.g.-mainframe, UNIX server, Windows server, AS/400, PC, laptop, Macintosh, PDA, cell phones, USB devices, etc.)
- b. Nature of the evidence maintained on the specific system (documents, databases, e-mail, etc.)

**18. Determine and identify what protocols should govern production with respect to logistics such as:**

- a. Tracking status?
- b. Media labeling?
- c. Bates numbering?
- d. Problem resolution (empty CD's, unreadable media, read errors, etc.)?
- e. Provenance information that accompanies media (what user/system/etc.)?

FOOTE, MEYERS, MIELKE & FLOWERS, LLC

19. Determine and identify what types of data may require special handling or additional research.

20. Discuss special redaction and privilege issues, such as but not limited to:

- a. Log files identifying information withheld as privileged and the nature of the privilege asserted?
- b. Special protection for trade secret and other intellectual property.
- c. Anonymity considerations for personal information.

**B. ESI and DOCUMENTS**

ESI is afforded the broadest possible meaning, and for purposes of this litigation, includes (by way of example and not as an exclusive list) potentially relevant information electronically, magnetically, optically, or otherwise stored as:

- Digital communications (e.g., e-mail, voice mail, instant messaging);
- E-Mail Server Stores (e.g., Lotus Domino .NSF or Microsoft Exchange .EDB);
- Word processed documents (e.g., Word or WordPerfect Files and drafts);
- Spreadsheets and tables (e.g., Excel or Lotus 123 worksheets);
- Accounting Application Data (e.g., QuickBooks, Money, Peachtree data);
- Image and Facsimile Files (e.g., .PDF, .TIFF, .JPG, .GIF images);
- Databases (e.g., Access, Oracle, SQL Server data, SAP);
- Contact and Relationship Management Data (e.g., Outlook, ACT!);
- Sound Recordings (e.g., .AVI and .MOV files)
- Presentations (e.g., PowerPoint, Corel Presentations)
- Network Access and Server Activity Logs;
- Video and Animation (e.g., .AVI and .MOV files);
- Calendar and Diary Application Data (e.g., Outlook PST, blog entries);
- Online Access Data (e.g., Temporary Internet Files, History, Cookies);
- Project Management Application Data;
- Computer Aided Design/Drawing Files;
- Active Files; and
- Backup and Archival Files (e.g., Veritas, Zip, .GHO)

ESI resides not only in areas of electronic, magnetic and optical storage media reasonably accessible to you, but also in areas you may deem not reasonably accessible. You are obligated to preserve potentially relevant evidence from both sources of ESI, even if you do not anticipate producing such ESI

Further, for purposes of this litigation the term "DOCUMENT" has the broadest meaning accorded that term by Rule 34 of the Federal Rules of Civil Procedure and Rule 26 of the Federal Rules of Evidence, and includes, but is not limited to, any kind of written or graphic material, however produced or reproduced, of any kind or description,



## FOOTE, MEYERS, MIELKE &amp; FLOWERS, LLC

whether sent or received or neither, including originals, copies, drafts and both sides thereof, and including, but not limited to: papers, reports, books, book accounts, photographs, tangible things, correspondence, reports and recordings of telephone conversations, telephone logs, statements, summaries, opinions, agreements, ledgers, journals records of accounts, checks, summary of accounts, spreadsheets, databases, receipts, balance sheets, income statements, confirmation slips, questionnaires, desk calendars, appointment books, diaries, journals, graphs, test results, blog, charts, data files, log files of computer access and activity, and all of the records kept by electronic, photographic, optical, mechanical, magnetic means and things similar to any of the foregoing, including computer media, regardless of their author.

C. PRESERVATION OF RELEVANT ESI AND DOCUMENTS

In order to ensure that relevant and discoverable information is available for later use, Plaintiff respectfully reminds you and your client of your obligations under the federal rules to preserve all relevant electronic data. *China Ocean Shipping (Group) Co. v. Simone Metals Inc.*, 1999 WL 966443, at \*3 (N.D.Ill. Sept. 30, 1999); *Byers v. Illinois State Police*, No. 99 C 8105, 2002 WL 1264004, at \*10 (N.D.Ill. June 3, 2002).

Under the federal discovery rules, a potential defendant has an obligation to begin preserving relevant evidence when litigation is reasonably foreseeable. *China Ocean Shipping (Group) Co.*, 1999 WL 96643, at \*3; *Cohn v. Taco Bell Corp.*, No. 92 C 5852, 1995 WL 519968, at \*5 (N.D.Ill. Aug.30, 1995). As counsel to our clients, we as attorneys have an ethical obligation to inform, advise, and assist our clients with preserving evidence. "When a lawyer who has been retained to handle a matter learns that litigation is probable or has been commenced, the lawyer should inform the client of its duty to preserve potentially relevant documents in the client's custody or control and of the possible consequences of failing to do so." Standard 10, *Preservation of Documents*, ABA Civil Discovery Standards (Aug. 2004). This letter is intended to firmly remind you and your client of your obligations to retain all relevant documents, communication, and electronic information.

Your client may have established data retention/destruction policies, and may currently be following those established schedules and procedures. **These procedures may be destroying important evidence which comprises the claims and defences of the parties; and, even if the destruction protocol has been established prior to when this litigation was reasonably foreseeable, such inadvertant destruction of relevant evidence may give rise to serious sanctions.** *Diersen v. Walker*, No. 00 C 2437, 2003 WL 21317276, at \*5 (N.D.Ill. June 6, 2003). Therefore, I urge your client to immediately suspend any activities which result or could result in the destruction of any ESI or Documents until the Rule 26(f) Conference is completed and an agreement is reached between the parties regarding the protection and preservation of relevant ESI and Documents.

## FOOTE, MEYERS, MIELKE &amp; FLOWERS, LLC

Preservation of all relevant documents, information, and data, will expedite the resolution of this action and simplify the discovery process. Furthermore, a failure to preserve this information may lead to the destruction of data essential to your client's defense. In sum, successful retention of relevant information benefits all parties. I am informing you of these specific intentions now so that your client can take the affirmative steps necessary to preserve this information and prevent its intentional or unintentional destruction.

Plaintiff anticipates the following categories of ESI, documents, data, and information as relevant to the alleged claims, and requests preservation of these, and any other categories of potentially relevant documents:

- **All E-Mail relevant to this litigation.** All electronic mail, electronic correspondence, or electronic peer-to-peer messages (e-mail") shall be produced in electronic form, in an accessible standard format, and on industry-standard computer media along with files included as attachments to such e-mail. Back-up archival copies of e-mail and e-mail attachments shall be restored as necessary to create a comprehensive collection of e-mail. No modification, alterations, or additions to e-mails (or to the meta-data and attachments associated with such e-mails) from their original states shall be performed. All e-mail should be produced whether:
  - Residing in active files on enterprise servers
  - Stored in active files on local or external hard drives and network shares
  - Nearline e-mail
  - Offline e-mail stored in networked repositories
  - E-mail residing on remote servers
  - E-mail forwarded and carbon copied to third-party systems
  - E-mail threaded behind subsequent exchanges
  - Offline local e-mail stored on removable media (external hard drives, thumb drives and memory cards; optical media: CD-R/RW, DVD-R/RW, Floppy Drives and Zip Drives)
  - Archived E-mail
  - Common user "Flubs"
  - Legacy e-mail
  - E-mail saved to other formats (.pdf, .tiff, .txt, .eml, etc.)
  - E-Mail contained in review sets assembled for other litigation/compliance purposes
  - E-Mail retained by vendors or third-parties
  - Print outs to paper
  - Offline e-mail on server back up media (Back up tapes, DLT, AIT, etc.)

FOOTE, MEYERS, MIELKE & FLOWERS, LLC

- E-mail in forensically accessible areas of local hard drives (deleted e-mail, internet cache, unallocated clusters)
- Proprietary software used to perform redaction.
- Commercial software used to perform redaction.
- Meta-data used to describe backup and archival media.
- Meta-Data used to identify computer systems relevant to this litigation.
- Meta-Data used to identify computer access relevant to this litigation.
- Complete history, records, and/or files related to Adwords and AdSense Programs
- The name and address of each and every participant in the Adwords and AdSense program
- The domain address of every participating domain in the AdWords and AdSense Programs
- Any and all documents, data, and information pertaining to registration and licensing domain names through the Google Adwords and AdSense Programs
- Any and all documents, data, and information pertaining to domain name research for the Google Adwords and AdSense Programs
- Any and all documents, data, and information pertaining to any and all subsidiaries and parent companies of all Defendants
- Any and all documents, data, and information pertaining to domain tasting and/or domain kiting
- Any and all documents, data, and information pertaining to domain name auction systems
- Any and all documents, data, and information pertaining to methods used to determine domain names
- Any and all documents, data, and information pertaining to typosquatting

FOOTE, MEYERS, MIELKE & FLOWERS, LLC

- Any and all documents, data, and information pertaining to “Google Domain Park”
- Any and all documents, data, and information pertaining to Google’s Semantic Technology
- Any and all documents, data, and information pertaining to Google’s domain reporting and portfolio analysis programs
- Any and all documents, data, and information pertaining to Google’s categories of revenue generating domain names
- Any and all documents, data, and information pertaining to Google’s traffic redirection programs and/or stealth redirection programs
- Any and all documents, data, and information pertaining to proprietary XML feeds
- Any and all documents, data, and information pertaining to the sites [www.google syndication.com](http://www.google syndication.com) and/or [www.applied semantics.com](http://www.applied semantics.com)
- Any and all documents, data, and information pertaining to Defendants’ individual and collective attempts to monitor and review every site for trademark infringement
- Any and all profit sharing agreements between Defendants
- Any and all documents, data, and information pertaining to Defendant Google’s online tracking and reporting system
- Any and all documents, data, and information pertaining to Defendant Google’s “loyalty” program and/or “Exclusivity” program
- Complete statistics and/or activity reports for all participating domain names
- Any and all documents, data, and information pertaining to domain parking conferences
- Any and all documents, data, and information pertaining to Defendants’ usage of the website [www.whois.com](http://www.whois.com)
- Any and all documents, data, and information pertaining to Google’s “intelligent placement” programs

FOOTE, MEYERS, MIELKE & FLOWERS, LLC

- Any and all documents, data, and information pertaining to usage of infringing “www” domain names, “com” domain names, and/or “http” domain names
- Any and all documents, data, and information pertaining to Google’s quality/webmaster guidelines
- Any and all documents, data, and information pertaining to Google’s online complaint system
- Any and all documents, data, and information pertaining to the Uniform Domain Name Dispute Resolution Policy
- Any and all documents, data, and information pertaining to “collective reports”
- Any and all documents, data, and information pertaining to Google’s “efforts for greater transparency”
- Any and all documents, data, and information pertaining to Google’s Placement Performance Reports
- Any and all documents, data, other information, invoices, bills, and/or other accounting documents related to the AdWords or AdSense Programs
- Any and all documents, data, and information evidencing revenue generated from the AdWords and/or AdSense Programs
- Any and all documents, data, and information related to any contracts between any of the named Defendants.
- Any and all documents, data, and information
- All e-mails related to Plaintiff and/or deceptive domains (as defined in Plaintiff’s complaint)
- All documents related to Adwords and/or AdSense practices, procedures, and/or policies
- Any and all software programs related to Adwords and/or AdSense
- All software programs related to Defendant Google search programs

FOOTE, MEYERS, MIELKE & FLOWERS, LLC

- Any and all communications, documents, and or other information related to any complaints of trademark infringement, dilution, or other such related violations
- All training and educational seminars related to Adwords and/or AdSense
- All consultant reports related to Adwords and/or Ad Sense practices, policies, and/or procedures
- All documents related to administrative, local, state, and/or federal claims made against Defendant related to Adwords, AdSense, and/or trademark or "distinctive and valuable marks" (as defined in Plaintiff's Complaint)
- All statements of potential witnesses or persons interviewed in connection with this case
- Mirrored images as of this date of all hard drives from the computers of all persons involved with Adwords and mirrored images to any servers (including e-mail servers) to which these persons may have had access
- All current back-up tapes (or other media used to back-up) hard drives and servers
- All documents, data, and information related to Adwords and/or AdSense programs
- All documents, data, and information related to Defendant's income from Adwords and/or AdSense
- Any and all communications, documents, data, and/or information related to any actions by Defendant taken to address, mitigate, prevent, and/or stop the participation of deceptive domains in the AdSense for Domains program
- Any and all documents, communications, information, and or data related to the identity of and operations of the Google Network
- Any and all documents, communications, information, and or data related to the marketing and promotion of the Google Network, Google AdWords and Google AdSense programs
- The identify of each and every individual and entity that Defendant Google has made a payment to in connection with the Google AdSense program, the date of payment, method of payment, and amount of payment.

FOOTE, MEYERS, MIELKE & FLOWERS, LLC

- Every letter, e-mail, electronic message, and or other communication sent by Defendant Google to AdSense participants related to their participation in the Google AdSense program.
- Each and every document, communication, data, and/or information related to Defendant Google's selection of and placement of advertising through its Adwords and AdSense programs
- Any and all communications, data, and other information related to revenue generated through Defendant Google's cost-per-click/pay-per-click advertising programs
- Any and all information related to Defendant Google's policies, procedures, regulations, and guidelines related to and/or governing its cost-per-click/pay-per-click advertising programs
- Any e-mails related to trademark and/or copyright concerns or issues
- Any and all documents, communications, information, and/or data related to Defendant Google's process of approving participation in its marketing and advertising programs
- Any and all insurance agreements that may provide coverage for Defendant in this matter
- Any other documents, data, information, and materials that Defendant either intends to use in defense of Plaintiff's claims, at hearing in this matter, or that Defendant believes may be relevant and/or probative of the claims asserted in Plaintiff's complaint

Again, the above-list is not exhaustive, rather it is exemplary of the type and scope of discoverable information that Plaintiff expects Defendant to produce pursuant to Rule 26 and that Plaintiff will be seeking from Defendant under Rule 34. Plaintiff demands that all such documents be preserved.

**D. PRODUCTION PROTOCOL**

As a courtesy, and in preparation for our Rule 26(f) Conference, Plaintiff informs you that it will be seeking agreement to the following "Production Protocol," and seeking incorporation of the substantive terms of this agreement in the Rule 16 Scheduling Order:

1. Each individual piece of computer media produced must be clearly labeled with a unique media control or Bates number which is indelibly written on, or affixed to, both the media itself and any enclosure or case produced with the media. This label or marking will be affixed in a place and manner which does not obliterate



FOOTE, MEYERS, MIELKE & FLOWERS, LLC

any labeling on the original media, and which does not interfere with the ability to examine or use the media.

2. Electronic records and computerized information must be produced in an intelligible format or together with a technical description of the system from which they were derived sufficient to permit rendering the records and information intelligible. This description shall include, but not be limited to:
  - a. Except where redaction is required by law or privilege, any record, document or data item which was created on a computer or computer system must be produced on computer media in the original unredacted form in which it was created and/or maintained. For all such media produced, external labels on the media shall contain a unique tracking number which can be used to associate the media with appropriate identification for the computer(s) from which the copies of computer files were made, and the full names of the individuals or business units who used the computer so identified. A record shall also be maintained and produced which show how the information on the media was copied, and whether or not it is a complete and forensically accurate copy of the original.
  - b. For any electronic records, documents or data items produced, the producing party shall verify that it has modified its document retention policies in a manner that will ensure retention of the original records, documents and data items. These document retention policies shall include, without limitation, policies which automatically delete electronic mail or remove unused files, policies which permit overwriting of computer media for system backup functions, and similar policies.
3. Should the producing party seek to redact any document based on some limitation of discovery (including but not limited to a claim of privilege), the producing party shall supply a list of the documents for which such a limitation of discovery is claimed, indicating:
  - a. The claimed grounds for the redaction.
  - b. The nature of the redacted material (e.g., "trade secret").
  - c. A description of the exact process used for redaction.
4. Should the producing party seek to withhold any document based on some limitation of discovery (including but not limited to a claim of privilege), the producing party shall supply a list of the documents for which such limitation of discovery is claimed, indicating:
  - a. The identity of each document's author, writer, sender.



FOOTE, MEYERS, MIELKE & FLOWERS, LLC

- b. The identity of each document's addressee, or person for whom it was intended.
  - c. The date of creation or transmittal indicated on each document, or an estimate of that date, indicated as such, if no date appears on the document.
  - d. The general subject matter as described on each document, or if no such description appears, then some other description sufficient to identify the document.
  - e. The claimed grounds for the limitation of discovery (e.g., "attorney-client privilege")
5. All computer media must be properly packaged to ensure safe shipping and handling. If any piece of media produced is known to have any physical defect, electronic defect, damaged data, or is infected with any virus or other harmful software of any kind, it should be clearly labeled so that appropriate care can be taken during its examination.
  6. All computer media, which can be write protected should be write protected before production.
  7. All copies of computer files for production will be created in such a way as to preserve the original directory structure and any information about the files that is created and maintained by the operating system and the software used to create and maintain the information. This will include, but is not limited to, dates, times, authorship, and transmittal information.
  8. Electronic records and computerized information must be produced with sufficient information to permit identification of the producing agent and business unit responsible for the production. This information shall include, but not be limited to:
    - a. The name of the corporation of entity that is producing the information, along with information such as country, city, site, and department sufficient to uniquely identify the producing agent.
    - b. The name or identity of the specific server or computer system from which the backup was produced or information copied.
    - c. The name or identity of the specific server or computer system upon which the information was originally created, and the name of the individual who created and/or maintained the information.

FOOTE, MEYERS, MIELKE & FLOWERS, LLC

- d. The name or identity of the specific server or computer system upon which the information was maintained during the course of normal business, if different from the system where it was created.

**E. SUSPENSION OF ROUTINE DESTRUCTION**

You are directed to immediately initiate a litigation hold for potentially relevant ESI, documents and tangible things and to act diligently and in good faith to secure and audit compliance with such litigation hold. You are further directed to immediately identify and modify or suspend features of your information systems and devices that, in routine operation, operate to cause the loss of potentially relevant ESI. Examples of such features and operations include, but are not limited to the following:

- Purging the contents of e-mail repositories by age, capacity and/or other criteria;
- Re-use (“rotation”) of back up media containing e-mail
- Hardware and software changes which make ESI inaccessible;
- Replacing back up systems without retaining the means to read older media
- Utilization of wiping software and encryption
- Using data or media wiping, disposal, erasure or encryption utilities and/or devices;
- Overwriting, erasing, destroying, or discarding backup media;
- Re-assigning, re-tasking, re-imaging or disposing of systems, servers, devices and/or media;
- Running antivirus or other programs effecting wholesale metadata alteration;
- Releasing or purging online storage repositories;
- Using metadata stripper utilities;
- Disabling server, packet or local instant messaging logging; and/or,
- Executing drive or file defragmentation or compression programs.
- Selling, giving away or otherwise disposing of systems and media.

**F. GUARD AGAINST DELETION**

You should anticipate that your officers, employees or others may seek to hide, destroy or alter ESI. You must act to prevent and guard against such actions. Especially where company machines were used for internet access of personal communications, you should anticipate that users may seek to delete or destroy information they regard as personal, confidential or embarrassing, and in so doing, they may also delete or destroy potentially relevant ESI. This concern is not unique to you. It’s simply conduct that occurs with such regularity that any custodian of ESI and their counsel must anticipate and guard against its occurrence.

FOOTE, MEYERS, MIELKE & FLOWERS, LLC

**G. PRESERVATION OF BACKUP TAPES**

You are directed to preserve complete backup tape sets (including differentials and incrementals) containing e-mail, ESI, and/or any other related documents and data of for all dates during the relevant time frame set forth in the Complaint: 2000 to the present.

**H. ACT TO PREVENT SPOILATION**

You should take affirmative steps to prevent anyone with access to your data, systems, and archives (whether an employee, agent, officer, director, consultant, contractor, affiliate, or other) from seeking to modify, destroy or hide ESI network or local hard drives and on other media or devices (such as by deleting or overwriting files, using data shredding and overwriting applications, defragmentation, re-imaging, damaging or replacing media, encryption, compression, steganography or the like).

**I. SYSTEM SEQUESTRATION OF FORENSICALLY SOUND IMAGING**

As an appropriate and cost-effective means of preservation, you should remove from service and securely sequester the systems, media and devices housing potentially relevant ESI related to the claims asserted in Plaintiff's Complaint, including but not limited to the following:

- Data evidencing each and every cost-per-click/pay-per-click advertisement that has been placed on a site containing less than eighty percent content;
- The identity of each and every non-content domain and/or deceptive domain (as defined in Plaintiff's Complaint);
- Every participant in the AdSense for Domains Program;
- Every participant in the AdWords Program;
- All revenue generated from cost-per-click/pay-per-click advertising

In the event you deem it impractical to sequester systems, systems, media and devices, we believe that the breadth of preservation required dictates that forensically sound imaging of the systems, media and devices is expedient and cost effective. As we anticipate the need for forensic examination of one or more of the systems and the presence of relevant evidence in forensically accessible areas of the drives, we demand that you employ forensically sound ESI preservation methods. **Failure to use such methods poses a significant threat of spoliation and data loss.**

"Forensically sound ESI preservation" means duplication of all data stored on the

## FOOTE, MEYERS, MIELKE &amp; FLOWERS, LLC

evidence media while employing a proper chain of custody and using tools and methods that make no changes to the evidence and support authentication of the duplicate as a true and complete bit-for-bit image of the original. The products of forensically sound duplication are called, *inter alia*, "bitstream images" or "clones" of the evidence media. A forensically sound preservation method guards against changes to metadata evidence and preserves all parts of the electronic evidence, including deleted evidence within "unallocated clusters" and "slack space."

**Be advised that a conventional copy, backup or "Ghosting" of a hard drive does not produce a forensically sound image because it only captures active, unlocked data files and fails to preserve forensically significant data existing in, e.g., unallocated clusters and slack space.**

Each forensically sound image should be labeled to identify the date of acquisition, the person or entity acquiring the image and the system and medium from which it was obtained. Each such image should be preserved without alteration.

**J. PRESERVATION IN NATIVE FORM**

All ESI data will be sought in the form or forms in which it is ordinarily maintained (i.e., native format). Accordingly, you should preserve ESI in such native forms, and you should not employ methods to preserve ESI that remove or degrade the ability to search the ESI by electronic means or that make it difficult or burdensome to access or use the information.

You should additionally refrain from actions that shift ESI from reasonably accessible media and forms to less accessible media and forms if the effect of such actions is to make such ESI not reasonably accessible.

**K. METADATA**

You should further anticipate the need to disclose and produce system and application metadata and act to preserve it. System metadata is information describing the history and characteristics of other ESI. This information is typically associated with tracking or managing an electronic file and often includes data reflecting a file's name, size, custodian, location and dates of creation and last modification or access. Application metadata is information automatically included or embedded in electronic files, but which may not be apparent to a user including deleted content, draft language, commentary, collaboration and distribution data and dates of creation and printing. For electronic mail, metadata includes all header routing data and Base 64 encoded attachment data, in addition to the To, From, Subject, Received Date, CC and BCC fields.

*As you know, Metadata may be overwritten or corrupted by careless handling or improper preservation, including by moving, copying or examining the contents of*

FOOTE, MEYERS, MIELKE & FLOWERS, LLC

*files. You must take all possible action to avoid such spoliation, damage, and/or destruction of metadata.*

**L. SERVERS**

With respect to servers used to manage e-mail (e.g., Microsoft Exchange, Lotus Domino) and network storage (often called a "network share"), the complete contents of each user's network share and e-mail account should be preserved. There are several ways to preserve the contents of a server. If you are uncertain whether the preservation method you plan to employ is one that we will accept as sufficient, please immediately contact the undersigned.

**M. HOME SYSTEMS, LAPTOPS, ONLINE ACCOUNTS and OTHER ESI VENUES**

Though we expect that you will act swiftly to preserve data on office workstations and servers, you should also determine if any home or portable systems or devices may contain potentially relevant data. To the extent that you have sent or received potentially relevant e-mails or created or reviewed potentially relevant documents away from the office, you must preserve the contents of systems, devices and media used for these purposes (including not only potentially relevant data from portable and home computers, but also from portable thumb drives, CD-R/DVD-R disks and the user's PDA, smart phone, voice mailbox or other forms of ESI storage. ). Similarly, if you used online or browser-based e-mail accounts or services (such as Gmail, AOL, Yahoo Mail, etc.) to send or receive potentially relevant messages and attachments, the contents of these account mailboxes (including Sent, Deleted and Archived Message folders) should be preserved.

**N. ANCILLARY PRESERVATION**

You must preserve documents and other tangible items that may be required to access interpret or search potentially relevant ESI, including logs, control sheets, specifications, indices, naming protocols, file lists network diagrams, flow charts, instruction sheets data entry forms, abbreviation keys, user ID and password rosters and the like.

You must preserve passwords, keys and other authenticators required to access encrypted files or run applications, along with the installation disks, user manuals and license keys for applications required to access the ESI.

You must preserve cabling, drivers and hardware, other than a standard 3.5" floppy disk drive or standard CD or DVD optical disk drive, if needed to access or interpret media on which ESI is stored. This includes tape drives, bar code readers, Zip drives and other legacy or proprietary devices.

FOOTE, MEYERS, MIELKE & FLOWERS, LLC

O. PAPER PRESERVATION OF ESI IS INADEQUATE

As hard copies do not preserve electronic searchability or metadata, they are not an adequate substitute for, or cumulative of electronically stored versions. If information exists in both electronic and paper forms, you should preserve *both* forms.

P. AGENTS, ATTORNEYS, and THIRD PARTIES

Your preservation obligation extends beyond ESI in your care, possession or custody and includes ESI in custody of others that is subject to your direction and control. Accordingly, you must notify any current or former agent, attorney, employee, custodian and contractor in possession of potentially relevant ESI to preserve such ESI to the full extent of your obligation to do so, and you must take reasonable steps to secure their compliance.

Q. PRESERVATION PROTOCOLS

We are desirous of working with you to agree upon an acceptable protocol for forensically sound preservation and can supply a suitable protocol if you will furnish an inventory and description of the systems and media to be preserved. Alternatively, if you promptly disclose the preservation protocol you intend to employ, perhaps we can identify any points of disagreement and resolve them. A successful and compliant ESI preservation effort requires expertise. If you do not currently have such expertise at your disposal, we urge you to engage the services of an expert in electronic evidence and computer forensics. As we have already indicated, we wish to have both our experts present at our Rule 26(f) Conference to work cooperatively to secure an appropriate electronic preservation and discovery plan that is acceptable to the parties and the Court.

R. DO NOT DELAY PRESERVATION

We have indicated our desire to schedule the Rule 26(f) conference and prepare a draft Rule 16 order, at your earliest convenience. **Do not defer preservation steps pending such discussions, as critically important ESI may be lost or corrupted as a consequence of delay.** Should your failure to preserve potentially relevant evidence result in the corruption, loss or delay in production of evidence to which we are entitled, such a failure would constitute spoliation of evidence, and we will not hesitate to seek sanctions.

S. IDENTIFICATION OF CUSTODIANS

Be advised that for each custodian of ESI or tangible documents that may be relevant to this litigation, Plaintiff seeks the name, last known address, position, dates of employment, association (contractor, employee, director, third party, etc.), description of ESI or tangible documents in custodian's possession, relevant dates, and media in which



FOOTE, MEYERS, MIELKE & FLOWERS, LLC

the ESI or tangible document is stored. Provide each custodian with written notice of the litigation hold and directives regarding the preservation protocol.

**T. CONFIRMATION COMPLIANCE**

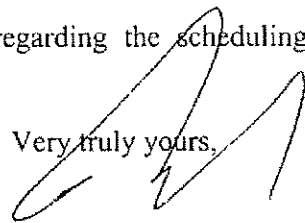
Confirm by July 12, 2007, that you have taken the steps outlined in this letter to preserve ESI and tangible documents potentially relevant to this action. Further, please provide written confirmation of that all relevant current and former employees, affiliates, contractors, associates, and other individual(s) and/or entities have been advised of the litigation hold and the protocol for preservation of ESI and tangible documents potentially relevant to this action. Please provide us with the name of each individual and/or entity that was so advised and the date of notice. If you have not undertaken the steps outlined above, or have taken other actions, please describe what you have done to preserve potentially relevant evidence.

**U. DATES FOR RULE 26(f) CONFERENCE**

Be advised that we are available to for the Rule 26(f) conference on any of the following dates July 9<sup>th</sup>, 10<sup>th</sup>, 13<sup>th</sup>, 19<sup>th</sup>, 20<sup>th</sup>, 23<sup>rd</sup>, 30<sup>th</sup> or August 1<sup>st</sup>, 2<sup>nd</sup>, 13<sup>th</sup> or 14<sup>th</sup>. We propose holding the meeting at our office in Geneva, Illinois. We anticipate the conference taking at least four (4) hours, however we suggest reserving the entire day to discuss the numerous issues set forth herein. Please advise at your earliest convenience as to your availability. We believe that our meeting would be most productive if both parties had their respective IT experts in attendance at the Rule 26(f) conference. We further demand that you bring individual(s) who possess sufficient knowledge of your ESI systems, hardware, software, media, data retention and destruction policies, and the other various categories of ESI and discovery issues set forth herein, to meaningfully address ESI discovery issues and participate in the process of reaching an agreement regarding discovery/ESI production and preservation protocols.

We look forward to hearing from you regarding the scheduling of the Rule 26(f) conference.

Very truly yours,

  
Robert M Foote, Esq.