EXHIBIT A

ELYSIUM™
DIGITAL

617.621.3100
Two Oliver Street, 11th Floor
Boston, MA 02109
www.elys.com

Initial Report of Michael Perry on Review and Export of Information from Jeff Dunstan's Computer System

Scope

I was asked to review the forensic images of two hard drives from a computer used by Jeff Dunstan in connection with the *Dunstan et al v. comScore, Inc.* litigation as described in the October 23, 2013 Protective Order covering production of Jeff Dunstan's hard drive. I, and colleagues working at my direction, reviewed these images and exported various data and reports ("Retrieved Data") in accordance with the Protective Order.

This report details the "Retrieved Data" to be produced to counsel for the Defendant after review by Plaintiff's counsel for potential objections to such production.

Forensic Images

Two forensic images were sent to Elysium Digital ("Elysium") on October 25, 2013 from Edelson, LLC. Neither image is included in the Retrieved Data; they are described here as they are referenced elsewhere in this report and in the Retrieved Data files.

1. Image Name: EDEL-JDunstanP0
   Model: WDC WD2500AAJS-60M0A0
   Serial #: Not present in the imaging log files.
   Source Data Size: 238475MB
   Image Captured: 12/21/2011
   Imaging Tool: FTK Imager

2. Image Name: EDEL-JDunstanP1
   Model: ST3160815A
   Serial #: 9RA72A66
   Source Data Size: 152627MB
   Image Captured: 12/22/2011
   Imaging Tool: FTK Imager

Analysis Tools

For reference purposes, Elysium used the following software during its analysis:

- X-Ways Forensics v. 16
- AccessData Forensic Toolkit (FTK) v4
- AccessData FTK Imager
- Internet Evidence Finder v6.1
- Misc. system utilities

System Information – The following information was extracted from the Windows Registry:

- Computer Name:ACER-262DC2EBF3
- RegisteredOwner : Lori
- ProductName : Microsoft Windows XP
  CSDVersion : Service Pack 3
  ProductId : 76487-OEM-0011903-00100
  CurrentBuildNumber : 2600
  BuildLab : 2600.xpsp_sp3_gdr.091208-2036
  SoftwareType : SYSTEM
  SourcePath : C:\I386
  SystemRoot : C:\WINDOWS
  PathName : C:\WINDOWS
  InstallDate : Wed Sep3 23:58:03 2008 (UTC)
- Logon Profile:"Lori"
  Last Updated: Wed Dec 21 20:40:54 2011 (UTC)
- Time Zone:
  DaylightName -> Pacific Daylight Time
  StandardName -> Pacific Standard Time

Retrieved Data

1. **File Listings** – File listings were created to include all files found in the forensic images. These files can be found in the "Filelists" directory. The files included are:

   - ES01_EDEL-JDunstan_FileList_Email.xlsx – This report contains all email files found in the forensic images. The report was compiled using FTK v4.
   - ES01_EDEL-JDunstan_FileList_Files.xlsx – This report contains all files found in the

forensic images, excluding email messages. The report was compiled using X-Ways Forensic v16.

2. **Windows Registry** – The Windows Registry hives were extracted from the forensic images and included in the "Registry-Natives" directory. The files included are: default, sam, security, software, system, and userdiff found at the path "\Windows\system32\config"; and ntuser.dat found at the path "\Documents and Settings\Lori\".

3. **Windows Registry – Extracted Data** - Data was extracted from each registry hive into text files, creating a human-readable version of the registry data. These files were named for the registry hive from which they were created (default.reg.txt, sam.reg.txt, security.reg.txt, software.reg.txt, system.reg.txt, userdiff.reg.txt, and ntuser.reg.txt) and saved in the "Registry-Extracted" directory.

4. **Event Logs** – All Windows event logs containing data were extracted from the forensic images as found at the path "\Windows\system32\config" and included in the "Event-Logs_Natives" directory. The files included are: AppEvent.evt, OSession.evt, and SysEvent.evt.

5. **Event Logs – Extracted Data** - All data was extracted from each event log into text files, creating a human-readable version of the event log data. These files were named for the event log from which they were created (AppEvents_exported.xlsx, OSession_exported.xlsx, and SysEvent_exported.xlsx) and saved in the "Event-Logs-Extracted" directory.

6. **Internet History** – Internet history artifacts were extracted from the forensic images using Internet Evidence Finder (IEF) v6.1. These reports were saved to the "Internet-History-Extracted" directory.

   These reports include:

   - Browser Activity.csv
   - Chrome Web History.csv
   - Chrome-360 Safe Browser Carved Web History.csv

- Firefox Bookmarks.csv
- Firefox Cache Records.csv
- Firefox Carved Web History.csv
- Firefox Downloads.csv
- Firefox FormHistory.csv
- Firefox Web History.csv
- Internet Explorer Cache Records Carved.csv
- Internet Explorer Cache Records.csv
- Internet Explorer History.csv
- Internet Explorer Leak Records.csv
- Opera Web History.csv
- Parsed Search Queries.csv

7. **Log Files –** Log files found in the forensic images were extracted and included in the "Log-Files" directory. The original path of these files was recreated in the "Log_Files" directory.

   The "Log-Files" directory also includes a file "MBAM-log-2013-10-30 (09-25-44).txt", which is a log file created by Malwarebytes as the result of a scan against the forensic images.

Retention of Copies of Forensic Images

In accordance with an agreement between the parties, Elysium Digital will retain the copies of the forensic images made for the analysis and in the production of the "Retrieved Data". These forensic images will be stored in a secure location at Elysium's office, and will not be reviewed or shared, unless by mutual agreement of the Parties, or an order from the Court.

The original image provided to Elysium will be returned to counsel for the Plaintiff with this report.

SIGNED UNDER THE PENALTY OF PERJURY THIS 31st day of October, 2013.

Michael Perry