

1 BINGHAM McCUTCHEN LLP
CHRISTOPHER B. HOCKETT (SBN 121539)
2 GEOFFREY M. HOWARD (SBN 157468)
ZACHARY J. ALINDER (SBN 209009)
3 BREE HANN (SBN 215695)
Three Embarcadero Center
4 San Francisco, CA 94111-4067
Telephone: (415) 393-2000
5 Facsimile: (415) 393-2286
chris.hockett@bingham.com
6 geoff.howard@bingham.com
zachary.alinder@bingham.com
7 bree.hann@bingham.com

8 DORIAN DALEY (SBN 129049)
JEFFREY S. ROSS (SBN 138172)
9 500 Oracle Parkway
M/S 5op7
10 Redwood City, CA 94070
Telephone: (650) 506-4846
11 Facsimile: (650) 506-7114
dorian.daley@oracle.com
12 jeff.ross@oracle.com

13 Attorneys for Plaintiffs
14 Oracle Corporation, Oracle USA, Inc.,
and Oracle International Corporation

15 UNITED STATES DISTRICT COURT
16 NORTHERN DISTRICT OF CALIFORNIA
17 SAN FRANCISCO DIVISION
18

19 ORACLE CORPORATION, a Delaware
20 corporation, ORACLE USA, INC., a Colorado
corporation, and ORACLE INTERNATIONAL
21 CORPORATION, a California corporation,

22 Plaintiffs,

23 v.

24 SAP AG, a German corporation, SAP
AMERICA, INC., a Delaware corporation,
25 TOMORROWNOW, INC., a Texas corporation,
and DOES 1-50, inclusive,

26 Defendants.
27
28

No. 07-CV-1658 EMC

**DECLARATION OF KEVIN
MANDIA IN SUPPORT OF
ORACLE'S MOTION FOR INTERIM
PRESERVATION ORDER AND
MEET AND CONFER SCHEDULE
FOR FINAL PRESERVATION
ORDER**

Date: June 6, 2007

Time: 10:30 a.m.

Judge: The Honorable Edward M. Chen
Courtroom C, 15th Floor

1 I, Kevin Mandia, declare:

2 1. I am CEO and president of Mandiant Corporation, a computer forensics and
3 information security consultation firm. I have a Master of Science degree in computer forensics
4 from The George Washington University and am a Certified Information Systems Security
5 Professional. For fourteen years, I have worked with electronic data investigations, computer
6 forensics, and information security, including conducting investigations for the Department of
7 Defense and for the Air Force Office of Special Investigations. I lecture in computer forensics at
8 Carnegie Mellon University, serve as adjunct professor of forensics at The George Washington
9 University, and have trained Assistant United States Attorneys and F.B.I. agents in computer
10 forensics. Except for matters stated below on information and belief, I have personal knowledge
11 of the matters stated in this Declaration by virtue of my retention by Oracle in this action. If
12 called and sworn as a witness, I could and would competently testify as to such matters.

13 2. Based on my review and understanding of Oracle's investigation and of its
14 records and data, as well as my experience with forensic computer investigations, I expect the
15 evidence in this case will consist almost entirely of electronically stored information. The
16 allegations in the Complaint describe SAP's practice of repeatedly using third parties' account
17 credentials to remotely access Oracle's support website. The Complaint further describes how
18 SAP then searched for and downloaded vast numbers of Software and Support Materials from
19 Oracle's website, regardless of the third parties' rights to such materials. Based on these
20 allegations, the categories of information that will be important for discovery will include the
21 actual Software and Support Materials that SAP downloaded from Oracle's website; information
22 related to those downloads, such as defendants' communications and internal records of the
23 means used to access the website; information related to SAP's storage of the downloaded
24 materials; and information related to the uses that SAP made of the downloaded materials –
25 including potentially providing them to its customers.

26 3. I expect that the overwhelming majority of evidence that falls into these
27 categories will consist of electronically stored information available on SAP's systems and
28 networks, including on its servers, computer drives, and other electronic storage media.. For

1 example, SAP's server and other network logs – computer-generated reports that reveal the
2 history of what data is placed onto and moved off of a particular computer or system – will detail
3 what materials were taken from Oracle's system, by whom at SAP, and by using which customer
4 credentials. These server and network logs will also demonstrate how SAP stored and used those
5 materials, as well as who had access to them. SAP's email records may reflect similar
6 information. As another example, the drives of SAP's computers may have records indicating
7 when SAP used those computers to access Oracle's systems, by whom, and by what means.

8 4. Electronically stored information, including server and network logs and other
9 kinds of electronic data and evidence, is dynamic and mutable by nature. Server logs for a
10 sophisticated enterprise with substantial internet activity will occupy a significant amount of
11 computer storage space. For this reason, many companies do not keep these logs for more than a
12 few days at a time in the ordinary course of business. Thus, some entries on network logs that
13 show particular download or transmission activity on a given day may only exist for short
14 periods of time. Moreover, since electronic records are frequently overwritten, deleted, or
15 modified during the normal course of business, this data is highly susceptible to inadvertent
16 alteration or destruction. Further, any internal inquiry or investigation performed without proper
17 forensic safeguards can impact the integrity of electronic evidence, including by materially
18 affecting, changing, or destroying evidence.

19 I declare under penalty of perjury under the laws of the United States of America
20 that the foregoing is true and correct.

21
22
23
24
25
26
27
28

Executed on April 30, 2007 in Alexandria, Virginia.

By: 
Kevin Mandia