

I, PETER GARZA, DECLARE:

I have personal knowledge of the facts recited herein and, if called and sworn as a witness, could and would competently testify thereto.

I. Qualifications

1. I studied computer science at National University and received a Business Administration Degree in 1988. I received my Masters of Science degree in Management Information Systems at Claremont Graduate University in 2001, and subsequently continued my studies there towards a Ph.D. in Information Systems. Between 1986 and 1999, I was employed with the Department of Defense as a criminal investigator. During that time period, I primarily worked as a special agent with the Naval Criminal Investigative Service and was responsible for conducting computer-related investigations. During the time I was employed the Department of Defense, I was given Top Secret clearance for Special Compartmented Information, the highest clearance available for the most sensitive information regarding counter-espionage and other top secret Department of Defense activities.

2. I have completed training courses in computer forensics, computer investigations and systems administration. I have developed and taught advanced training courses in computer crimes investigation for the Department of Defense and other Federal law enforcement agencies, including the Federal Bureau of Investigation and the Air Force Office of Special Investigations, as well as assisting other local law enforcement agencies in developing criminal computer investigation procedures. These courses also included instruction on advanced computer forensics and computer crimes investigation.

3. From 1991 through 1996, I specialized in the analysis and retrieval of electronic evidence for the Department of Defense. From 1996 through December 1999, I was responsible for conducting computer intrusion investigations and counter intelligence analysis on computer networks operated by the Department of Defense. During 1991-1999, I performed forensic analysis of more than 1000 computer systems. This analysis included the recovery of evidence from hard disk drives, many types of network servers, floppy disks, backup tapes, optical drives and other types of computer media. Both as an agent and later as a consultant, I have successfully recovered evidence

from enterprise computer systems that have spanned from palm-top devices to mainframes. The many types of servers involved in these cases have included databases, electronic mail, workgroup calendars, application servers, file servers and web servers.

4. From 1999 until the present, I have worked as an expert specializing in information technology investigations and the analysis and retrieval of electronic evidence. I have been involved as both an independent expert and a consulting expert performing electronic discovery in numerous cases, including those involving the theft of intellectual property, misappropriation of proprietary information and trademark infringement.

5. A true and correct copy of my resume is attached hereto as Exhibit A.

II. Data on Computer Systems

6. I have been involved in many large investigations, many of which involved classified information, that have included the identification, recovery and analysis of electronic records. An enterprise of any considerable size must have in place many computer systems and the mechanisms to share information. Electronic mail (email), databases, file servers, and other types of servers process individual transactions that, combined, are used to store and share knowledge within the organization. Individual users interact using desktop computers, laptop computers and other electronic devices that facilitate communication and the exchange of information. It has been my experience that even a single transaction, a piece of email with an attachment for instance, will originate with a user device, transit one or more servers on the way to its intended recipients and may leave several copies along the way. These copies may then be retrieved without damage to the user device or servers.

7. Copies of individual documents or transactions are made both interactively by the user and automatically by the software applications and computer operating systems the user utilizes. Simply editing and printing a word processing document from a floppy disk may create temporary copies on the hard disk drive of the computer. In addition, copies of individual transactions are memorialized for a time in server and workstation backups.

III. Electronic Discovery

8. Electronic records are particularly susceptible to alteration or destruction. Even under the best of circumstances, electronic data is lost during normal user activity. Temporary files created during editing or printing are overwritten by system or application software. System backup tapes are reused during normal rotation. In addition, even unsophisticated users have access to readily available tools to obliterate deleted information. When computer files are deleted, the data is still recoverable. The space used by a deleted file is not emptied, as one might think, it is marked for reuse. Until a new file takes all or a portion of that space, some extent of the data is recoverable. The first prudent step in the electronic discovery process should be to preserve data that may be lost through intentional or unintentional actions.

9. Taking backup tapes out of rotation or preserving individual personal computers until they are copied are steps routinely taken by a producing party. If, for example, an organization has the policy of overwriting or deleting daily backup tapes every 30 days, data on those tapes that have reached that threshold will be lost. Personal computers should be shut down and temporarily quarantined so that a proper backup can be made to freeze the data on the computer.

10. In addition to the primary content of electronic records, the text of a word processing document for instance, there is additional information about the document available that is unique to electronic records. Data that identifies when documents are created, modified, printed or even the author is often embedded in electronic documents. This data about electronic documents, known as metadata, may assist in resolving important issues in an investigation. Some forms of electronic documents and communications exist primarily or exclusively as electronic data. System logs, that track electronic communications, and electronic mail are two examples. It should be noted that simply printing these types of documents or large volumes of other general types of electronic documents may reduce their utility or make review unmanageable. Producing and reviewing tens of thousands or more electronic documents in printed format is unnecessarily burdensome. Thus, the more economical and efficient method to preserve and review electronic data is in creating and preserving those records in electronic copies.

11. Electronic data stored as files on computer disks as backups on data tapes or other media can be copied and reviewed in a number of different ways. Copies of computer disks can be accomplished by a logical backup or copy, which involves the normal mechanisms users employ to move data from one media to another, or an image copy which involves special tools to copy all regular files, remnant and deleted data. Electronic discovery routinely involves both logical or image copies of the producing party's computer media. Technical and practical protocols are usually put in place to ensure responsiveness and protect privilege of the data. Image backups of personal computers and servers can be accomplished with minimal disruption to an enterprise. Data maintained on backup tapes can be restored to other storage media for review.

12. Data obtained through the restoration of the producing party's own backups, forensic image backups of computers and logical copies of certain types of data are normally reviewed using a range of analysis and search tools. Forensic review should involve a combination of automated search and recovery tools and examiner review to identify responsive material. Computer forensic techniques are normally applied to both identify all responsive material and explain metadata, fragmentary data and remnant data.

IV. Information Systems Survey

13. In conjunction with requiring that the producing party protect responsive computer data, initial steps should involve identifying the relevant information systems of the producing party. Both technical and practical electronic discovery protocols will depend on the type, size and number of relevant computer systems. Quickly reaching an understanding of the relevant computer systems will minimize the disruption to the producing party and help protect the integrity of the data.

14. I have conducted research of public records available online via the Internet and have seen press accounts along with individual postings that indicate both Andersen and Enron Corporation likely use Lotus Notes in their enterprise. Lotus Notes is used for electronic mail, collaboration and obtaining access to disparate databases. Common sense, along with my experience with electronic discovery in large organizations along with the information available online indicates both organizations have large information systems that are likely to involve multiple database, email, application and other servers at each location in question. Both organizations exhibit sophistication

in information systems and it is likely there is much data that exists only in electronic format. Press accounts online and otherwise have described "Electronic Town Hall" meetings conducted by Enron CEO, Kenneth Lay. Instant messages or interactive online discussions, along with electronic mail and collaboration facilities inherent in group software such as Lotus Notes indicates the presence of much information that is likely to reside only in electronic format.

15. Outside sources only provide a glimpse into what the likely relevant systems may be. Interviews of appropriate information technology personnel, conducted in an appropriate setting, are necessary to facilitate identifying the relevant computer systems. Once all relevant information systems are identified, computer forensic techniques will be the most effective way to protect the integrity of the data, along with ensuring the production of responsive data is the most effective way.

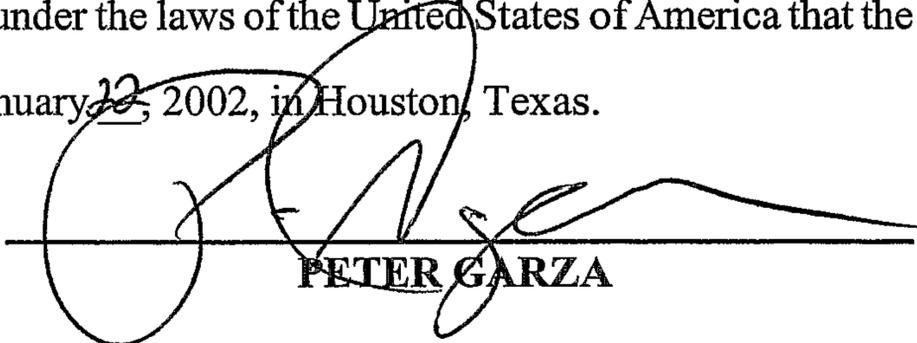
V. Proposed Steps for Electronic Discovery

16. Based upon my expertise and experience in computer forensics, computer investigations, and systems administration, the following steps may be taken that will efficiently and effectively preserve evidence relating to this action:

- (a) Perform information systems survey to identify relevant computer systems.
- (b) Execute a protocol for acquisition backup of electronic data.
- (c) Conduct forensic analysis of data to identify relevant data.
- (d) Preserve and safeguard data to prevent its loss and/or destruction.

17. Discovery of each type of system may involve a simple standard protocol, such as the quarantine, image backup, analysis and production of data from personal computers, or more involved individual protocols that depend on the specific systems operated by Andersen.

I declare under the penalty of perjury under the laws of the United States of America that the foregoing is true and correct, executed on January 22, 2002, in Houston, Texas.



PETER GARZA

EXHIBIT A



EvidentData
We Find Answers

Peter Garza

*President, CTO
EvidentData, Inc.
10621 Church Street
Suite 104
Rancho Cucamonga, CA 91730
Telephone: 909.948.7714
Telefacsimile: 909.948.4365
Email: pgarza@evidentdata.com*

PROFESSIONAL HISTORY

Mr. Garza is an experienced computer forensics consultant. Prior to founding Evidentdata, Inc., Mr. Garza conducted and supervised computer related investigations for over ten years as a Special Agent with the Naval Criminal Investigative Service. During that time Mr. Garza recovered and analyzed an array of computer generated evidence including electronic business records used to expose defense procurement fraud and residual computer files used in criminal and counterintelligence investigations. Mr. Garza has used his extensive experience to build a computer forensics training facility and laboratory with the capacity to work the most challenging cases.

Mr. Garza is a recognized expert in conducting real-time network incident response and on site remediation. Mr. Garza has also had extensive experience recovering electronic records generated in networked environments using Novell, DEC, Sun Microsystems, Windows NT and other operating environments.

Case Examples

- **Internet Investigations** - Prepared and executed the first court-ordered wiretap on an Internet connected network that exposed an Argentine computer hacker using Harvard University's network to compromise research facility computer networks at DoD, NASA, and around the world. The case was announced by Attorney General Janet Reno in March, 1996.
- **Computer Incident Remediation** - Investigated and identified network-based attacks and designed comprehensive network remediation plans.
- **Computer Forensics** - Applies extensive experience in recovering evidence from information systems when assisting client law firms obtain useable evidence from computers. Experienced investigator's approach has helped win civil litigation cases.
- **Electronic Documents Discovery** - Extensive experience in the recovery, review and production of data from information systems. Has been appointed as expert to facilitate the review of large amounts of electronic records to determine privilege and responsiveness to court orders.
- **Fraud Investigations** - Managed complex fraud investigations involving information technology audits, technical interviews, recovery of documentary and electronic evidence, and presentation of technical information for court proceedings.
- **Corporate Competitive Intelligence** - Conducted network analysis

Peter Garza
(Continued)

for organizations seeking to reveal attempted computer intrusions, possible theft of proprietary information and quantification of a competitor's efforts to obtain company information.

- Intellectual Property Protection – Planned and executed comprehensive investigative support for litigation involving the theft of trade secrets. Used comprehensive analysis techniques to expose and trace electronic theft of proprietary information by departing employees.

EDUCATION

MSMIS, Claremont Graduate University
BBA, National University

RESEARCH

Continuing studies towards a Ph.D. in information systems. Research areas include information security, the application of systems analysis techniques to the investigative process, information systems auditing and training of computer security professionals

TRAINING

Investigative and computer evidence courses completed include: criminal investigations courses, advanced interviewing courses, IACIS Computer Seizure Course, network intrusion detection courses, Novell Networking Technologies, UNIX system administration courses, the Telecommunications Fraud Training Program (FLETC), and the Computer Evidence Analysis Training Program (FLETC.)

PROFESSIONAL MEMBERSHIPS

President, High Technology Crime Investigation Association
Southern California Chapter (Los Angeles)

Member, International Association of Computer Investigative Specialists

Peter Garza, President, Evidentdata, Inc.

The following is computer security, system administration and computer investigations training I have designed, published and presented.

January 2001 - Present

“Practical Forensics: Managing IT Investigations” course taught for the Computer Security Institute, San Francisco, California at various locations

“Technical Recovery in Electronic Evidence” course taught for the Computer Security Institute, San Francisco, California at various locations

September 1999

“Network Investigations” presentation for the High Tech Crime Investigators Association International Conference, San Diego, California.

June 1999

“The Virtual Crime Scene” presentation for the Forum of Incident Response and Security Teams International Conference, Monterrey, Mexico.

February 1999

“Conducting International Investigations” and “Investigating Related Crime” presentations at a training conference hosted by the Federal Law Enforcement Training Center, Financial Fraud Division in Saint Petersburg, Russia.

February 1998

“Unix System Administration Course for Investigators” training course taught for The Naval Criminal Investigative Service and Marine Corps Computer Sciences School

1997 - 1998

“Network Intrusion Detector” training course hosted by the Naval Criminal Investigative Service and certified by Lawrence Livermore National Laboratory

1997 - 1999

Regular guest speaker on network security and incident response for a Information System Security Manager manager at the Marine Corps Computer Sciences School

1995 - 1997

“Hackers, Crackers and Sniffers” course on hacker investigations. Presentations on investigating computer intrusion incidents, New Dimensions International, various locations for NASA, AFOSI, Naval Research Laboratory, and the Defense Intelligence Agency

Spring 1996

"Investigative Incident Response: More than Just the Facts" invited presentation to System Administration and Network Security conference, Baltimore, Maryland

December 1994

Federal Computer Investigation Committee conference
"Search and Seizure of Novell Netware Servers"