

**IN THE TWELFTH JUDICIAL CIRCUIT  
IN AND FOR MANATEE COUNTY, FLORIDA  
CIVIL DIVISION**

MARY LOU SMITH  
an individual, and  
SHARON DENSON,  
an individual

Plaintiffs,

vs.

CASE NO: 2008-CA-11315

TRAILER ESTATES PARK AND  
RECREATION DISTRICT,  
an independent special taxing district,  
JANET JONES, an individual,  
JOHN VANDERMOLEN, an individual,  
JOSEPH SALERNO, an individual, and  
MARY LOU MCNULTY, an individual

Defendants.

FILED IN OPEN COURT  
THIS 5 DAY OF FEB 2010  
R.B. SHORE, CLERK  
BY *[Signature]* DC

**AFFIDAVIT OF MATTHEW J. DECKER**

I, Matthew J. Decker, being duly sworn, states as follows:

1. I am over eighteen (18) years of age and have personal knowledge of the information contained within this affidavit.

2. I am an expert in information security and computer forensics with over twenty years of professional experience in the service of the United States Department of Defense (DoD) and private industry; serving Agile Risk Management LLC, KPMG LLP, Lucent Technologies, International Network Services, Booz Allen Hamilton in service to the United States Special Operations Command (USSOCOM), and over nine years with the National Security Agency (NSA). A copy of my curriculum vitae is attached as **Exhibit A**.

3. In the past 4 years, I have testified in court, as follows:

a. March 2007, Pharmacia, Inc. vs. Scott Arledge; Case No. 8:07-cv-486-T-26MAP; UNITED STATES DISTRICT COURT, MIDDLE DISTRICT OF FLORIDA, TAMPA DIVISION.

b. October 2008, Southeastern Mechanical Services, Inc. v. Norman Brody, et al; Case No. 8:08-cv-1151-T-30EAJ; UNITED STATES DISTRICT COURT, MIDDLE DISTRICT OF FLORIDA, TAMPA DIVISION.

c. December 2009, Kincaid Coach Lines, Inc vs. Debbie Van Pay, et al; Case No. 09004507CA; CIRCUIT COURT OF THE FOURTEENTH JUDICIAL CIRCUIT, BAY COUNTY, FL.

4. In the past 4 years, I have given deposition, as follows:

a. June 2007, BENEVIDES AND GERARD, P.A., and PRISCILLA GERARD, individually, vs. LOUIS BENEVIDES, individually and REBECCA NOONON, individually, Case No. GC07-76; CIRCUIT COURT OF THE TENTH JUDICIAL CIRCUIT, HIGHLANDS COUNTY, FL.

b. September 2008, Technology Conservation Group, Inc. v. MARS LLC, et al; Case No. 2008 CA 1755; CIRCUIT COURT OF THE FIFTH JUDICIAL CIRCUIT, CITRUS COUNTY, FL.

c. January 2010, Pegasus Imaging Corporation vs. Allscripts Healthcare Solutions, Inc, et al; Case No. 8:08-cv-1770-T-30 EAJ; UNITED STATES DISTRICT COURT, MIDDLE DISTRICT OF FLORIDA, TAMPA DIVISION.

5. I have been appointed as an independent expert by the courts, as follows:

a. September 2008, Court appointed Independent Forensics Expert in Southeastern Mechanical Services, Inc. v. Norman Brody, et al; Case No.: 8:08-cv-1151-T-30EAJ; UNITED STATES DISTRICT COURT, MIDDLE DISTRICT OF FLORIDA, TAMPA DIVISION.

b. November 2009, The Raymond F. Kravis Center for the Performing Arts, Inc., vs. Lexington Insurance Company, et al, Case No.: 2005 CA 2274 AH; CIRCUIT COURT OF THE FIFTEENTH JUDICIAL CIRCUIT, PALM BEACH COUNTY, FL.

6. I have reviewed excerpts of the depositions of Jones, McNulty, VanderMolen, Brauer, Durham, Fitzpatrick, Opper, and Miller. A computer forensics examination of the computers used by these individuals can be conducted in a minimally intrusive manner in order to confirm or deny whether all responsive data on the computer has been produced. Recovering deleted email from computers is common place. Several of the individuals have testified to deleting emails and documents and/or that their computers routinely delete emails. Other artifacts, like Word documents and spreadsheets, are often even more easily recovered than email.

7. On numerous occasions, including each of the cases referenced in para 5, above, I have been asked to prepare and/or execute protocols to address the preservation, collection, and analysis of electronically stored information (ESI) relevant to each matter. The purpose of these protocols is, in general, to ensure that appropriate ESI relevant to the matter is presented to the opposing party, while ensuring that ESI containing privileged material is explicitly restricted from examination by the opposing party.

8. An effective protocol will address the following, at a minimum:

- a. The scope of the inspection, detailing the specific devices or locations from the available universe of ESI upon which the inspection will be performed.
- b. The manner in which the ESI is to be preserved and collected, thus permitting inspection results to be repeatable. How the ESI is preserved and collected is also critical to ensuring that the data “type” of interest is available for inspection. The data “type” generally falls into one of three categories:
  - i. Active Data is information typically seen by a computer user, such as data files, programs, and files used by the operating system. This is typically the easiest type of data to obtain.
  - ii. Latent Data is information that typically refers to deleted, partially overwritten, file slack, or other data that generally require specialized tools for inspection and analysis.
  - iii. Archival Data is data that has been backed up and stored, which may consist of backup tapes, CD's, DVD's, etc.
- c. Who is to conduct the inspection.
- d. How the data will be inspected. The manner in which the ESI is to be inspected may include via keyword searches to identify potentially relevant data, searching within selected file types (e.g. Word documents, email, archive files, etc), registry analysis, log file analysis, data associated with relevant time periods, etc.

Establishing how the ESI is to be inspected defines permissible actions that can be taken upon the data during the examination and thus ensures a minimally invasive investigative process.

e. The process by which privileged versus non-privileged ESI is identified and produced to the opposing party. This typically involves a review of the data produced in the course of the inspection by Counsel of the producing party. Counsel prepares a privilege log of data not to be produced to opposing Counsel, and the forensic examiner presents only the non-privileged data to opposing Counsel.

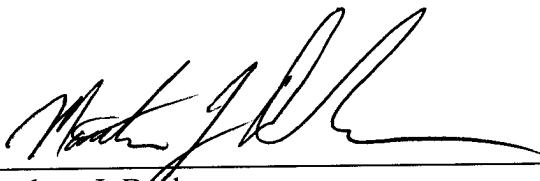
9. The need to produce specific and relevant ESI from data storage locations containing a mixture of privileged and non-privileged information occurs frequently, and is commonly addressed via the services of qualified digital forensics practitioners. This case is not unique in this regard, and an appropriate protocol can be developed to preserve, collect, analyze and produce the non-privileged information from the ESI universe of the Defendants such that Plaintiffs can obtain the discovery information to which they are entitled.

10. The foregoing is true and correct.

11. This ends my affidavit.

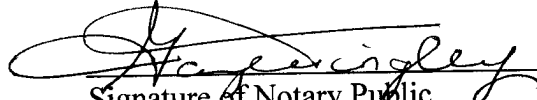
**FURTHER AFFIANT SAYETH NOT.**

Dated this 3 day of February, 2010.

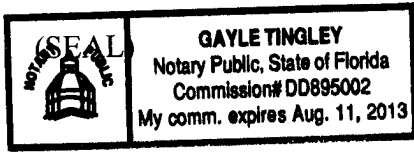
  
\_\_\_\_\_  
Matthew J. Decker

STATE OF FLORIDA                    )  
COUNTY OF HILLSBOROUGH        )

The foregoing instrument was acknowledged before me this 3 day of February, 2010,  
by Matthew J. Decker. He is personally known to me or has produced FL DL as  
identification.

  
Signature of Notary Public,  
State of Florida

My Commission Expires: Aug 11, 2013



## **Exhibit A – Matthew Decker CV**

Curriculum Vitae for Matthew J. Decker



**Matthew Decker, DFCP, CIFI, CISSP, CISA, CISM**  
Principal  
Agile Risk Management LLC  
Private Investigative Agency, Lic# A2700080  
Web: [www.AgileRiskManagement.com](http://www.AgileRiskManagement.com)  
E-mail: [mjdecker@agilerm.net](mailto:mjdecker@agilerm.net)  
(O) 877.244.5313

### **Summary**

Matthew Decker, a principal with Agile Risk Management LLC since January 2004, is an expert in information security and computer forensics. He has over twenty years of professional experience in the service of the United States Department of Defense (DoD) and private industry. During his career he has delivered his services with KPMG LLP, Lucent Technologies, International Network Services, Booz Allen Hamilton in service to the United States Special Operations Command (USSOCOM), and over nine years with the National Security Agency (NSA). He is experienced in delivering a wide variety of services including security audits, post incident response & forensic analysis, risk analysis, penetration testing, vulnerability assessments, secure infrastructure design, and corporate policy review & development. Mr. Decker received his Bachelors Degree in Electrical Engineering (BSEE, Florida Atlantic University) in 1985, and earned a Masters degree in Business Administration (MBA, Nova Southeastern University) in 1998. NSA's Engineering and Physical Science Career Panel awarded him Certified Cryptologic Engineer (CCE) stature in 1992. He is a member in good standing of ISSA, ISACA, InfraGard and the IISFA, and served as President to the Tampa Bay Chapter of ISSA from 1999 - 2003. Matthew holds numerous professional security certifications, is published in the ISSA Journal, is published in the Information Security Management Handbook (5th edition, Volumes I & II), and is a frequent speaker at computer security related events.

### **Computer Forensics Highlights**

Mr. Decker has satisfied numerous court orders for evidence collection, preservation & analysis, and is an experienced expert witness. He is fluent with numerous forensics tools including the widely known EnCase and FTK applications, and joins in holding patent-pending status for state-of-the-art forensics capabilities developed exclusively by Agile Risk Management LLC.

### **Professional Memberships & Certifications**

PI (Private Investigator, State of Florida; Lic# C2700154)  
DFCP (Digital Forensics Certified Practitioner)  
CIFI (Certified Information Forensics Investigator)  
CISSP (Certified Information Systems Security Professional)  
CISA (Certified Information Systems Auditor)  
CISM (Certified Information Security Manager)  
NSA-IAM Certified (National Security Agency InfoSec Assessment Methodology)  
National Security Agency (NSA) Certified Cryptologic Engineer  
President of the ISSA Tampa Bay Chapter (1999-2003)  
Member in good standing of ISSA (Information Systems Security Association), ISACA (Information Systems Audit and Control Association), InfraGard (FBI sponsored organization), and IISFA (International Information Systems Forensics Association)

**Agile**  
Risk Management LLC