EXHIBIT G

Attachment A

KEVIN MANDIA

President and CEO

kevin.mandia@mandiant.com

675 N Washington Street
Alexandria, VA 22314
phone (800) 647-7020
fax (703) 683-2891

ACCOMPLISHMENTS

As CEO and President of Mandiant Corporation, Kevin has grown a profitable, self-funded consulting firm to over 90 employees in approximately six years.

Kevin is a computer forensics expert who has provided forensic analysis and support in *United States v. Sami Omar Al-Hussayan, United States v. Vasily Gorshkov, United States v. Alexey Ivanov*, *United States* v. *Markus Lukawinsky*, *United States* v. *Bret McDanel*, *United States* v. *Kai Xu et al*, *United States* v. *Walter A. Forbes and E. Kirk Shelton*, and *United States* v. *Chad Grant.* He has testified as an expert in Federal Court for the United States Department of Justice on four separate occasions.

As a professorial lecturer at Carnegie Mellon and The George Washington University, Kevin has taught the most advanced graduate level course on Incident Response and computer forensics at both schools.

He has a national reputation as a trainer, instructor, and lecturer in computer forensics and incident response. As the author of two computer forensics books, Kevin has lectured at dozens of national level conferences, including: BlackHat, RSA Conference, Networld+Interop, Infragard, High Technology Crime Investigation Association (HTCIA), SC Forum, and for the Information Systems Security Association (ISSA). Kevin has been interviewed for *The Washington Post*, *The New York Times, The Wall Street Journal, Forbes,* CNN Talkback Live, the Associated Press, Bloomberg News and various information security industry publications.

Kevin has provided professional training to hundreds of law enforcement and computer forensics experts, including professionals at Prudential, State Farm, the Federal Bureau of Investigations (FBI), the U.S. Air Force, Fidelity, Bell South, and many other firms or government agencies.

PROFESSIONAL EXPERIENCE

President and CEO, 2004 - Present
Mandiant Corporation, Alexandria, Virginia

- Founded an information security company offering professional services targeting proactive and reactive security initiatives including: computer forensics, incident response, network security, applications security, education and research and development.
- Testified twice as the computer forensics expert in Federal criminal court in a computer intrusion case in the Southern District of California. Performed computer forensic analysis of computer systems in support of the case *United States v. Grant*.
- Continually manages teams of technicians that respond to complex computer intrusions, from International hackers to state-sponsored intrusions.

Director 2003 – 2004
FTI Consulting, New York, New York

- Managed a team of computer forensic examiners.
- Provided computer forensics support for ongoing disputes.
- Led FTI's efforts in responding to computer security incidents.

Director of Computer Forensics, 2000 – 2003
Foundstone, Incorporated, Washington D.C.

- Created and managed Foundstone's Computer Forensics practice.
- Provided computer forensic support for seven criminal and over 20 cases.
- Supervised the Computer Forensics and Incident Response efforts of 30 Foundstone consultants.
- Expert hired for seven criminal cases, including theft of intellectual property and international computer intrusion cases.

- Expert hired by numerous law firms, including Fenwick & West, Kirkland & Ellis, Arnold & Porter, Bingham Dana, and Alston & Bird for civil litigation support.
- Testified twice as an expert in criminal Federal cases.
- Developed a 3-day computer investigations class for the U.S. Attorney's office.
- Trained over 50 Assistant U.S. Attorneys who specialize in prosecuting computer crime.
- Taught at the Department of Justice's National Advocacy Center.
- Developed two Continuing Legal Education Classes titled "Complying With Information Security Legislation and Standards to Reduce Liabilities" and "Understanding Cyber Attacks."
    - Trained over 100 attorneys.
    - Classes approved by the CLE boards in the States of Virginia, New York, and California (others pending) for 8.5 CLE credit hours. Content covers:
        - Gramm-Leach-Bliley Regulations for Financial Institutions
        - HIPAA Regulations for Health Organizations
        - FTC Regulations
- Developed a one-week computer forensics class for Prudential.
    - Class CFE approved and attendees attained 35 CFE credits.
- Created a one-week class entitled "Forensic Investigations of Computer Intrusion Cases" for the Royal Canadian Mounted Police and the U.S. Secret Service.
- Trained over 60 U.S. Secret Service Agents specializing in computer crime.
- Trained at the Royal Canadian Police College.
- Trained computer forensic specialists at TD Bank, Royal Bank of Canada, Fidelity, Prudential, State Farm, Southwestern Bell Communications, Microsoft, Bank One, General Electric, BB & T, and numerous other Fortune 500 firms.
- Performed over 30 computer intrusion and theft of Intellectual Property investigations for private corporations.
- Performed network attack and penetration testing for corporate clients.

Director of Training, Director of Information Security, 1998 - 2000
Sytex Incorporated, Columbia, Maryland

- Developed a two-week computer intrusion response course for the Federal Bureau of Investigation.
- Trained over 400 FBI agents specializing in computer intrusion cases.
- Supervised the efforts of five trainers and was responsible for all course content.
- Taught on-site at the FBI Academy at Quantico for over one year.
- Developed an advanced one-week computer intrusion investigators course for the FBI.
- Personally trained over 100 FBI agents in advanced computer intrusion investigations.
- Trained over 200 Air Force, State Department, CIA, and Office of the Inspector General's (OIG) computer crime intelligence analysts and criminal investigators.
- Selected by the FBI's National Infrastructure Protection Center, the Air Force Office of Special Investigations, and private corporations to investigate computer intrusion cases.
- Selected by the FBI to work on special network intrusion cases.

Special Agent, 1996 - 1998
The Air Force Office of Special Investigations

- Conducted more than 80 interviews while being involved in over 25 different investigations.
- Cases included fraud, theft, sex offenses, and Counter-intelligence matters.
- Involved in nearly 20 Computer Intrusion Cases.
- Deployed to interview system administrators and led install of wiretap software.
- Reviewed over 1,000 pages worth of computer intrusion logs.
- Wrote approximately five affidavits to obtain subscriber information from Internet Service Providers.
- Provided investigative support on computer related investigations to the FBI, Secret Service, CIA, NSA, INTERPOL, and other government and allied agencies.
- Assisted in the creation of Forensic Media Analysis Laboratory Procedural Guidelines for the Air Force Computer Forensics Lab.
- Testified in evidentiary hearing on computer forensic evidence.

Computers and Intelligence Programs Analyst, 1994 - 1996
Defense Information Systems Agency

- Headed development of corporate planning database system for the Defense Information Systems Agency's (DISA) $800 million appropriated and $2.1 billion Defense Business Operating Fund (DBOF)

programs.
- Provided expert support to manage DISA's financial database. Trained users, installed systems, and resolved trouble-calls to allow instant access for more than 200 users.
- First Lieutenant in the United States Air Force.

Computer Security Officer, 1993 - 1994
7th Communications Group, Pentagon, Washington D.C.

- As a Second Lieutenant, led a team of four computer security specialists responsible for computer security on three IBM mainframe computers in the Pentagon's $200 million dollar Central Computer Facility, processing classified information up to and including Top Secret.

PUBLICATIONS

- "Don't Forget Your Memory," *Forensic Magazine*, Kevin Mandia and Kris Harms, December 2007.
- "Dissecting the Damage of Hackers. Attorneys beware: Computer security breaches are no longer just an IT problem," *LegalTimes*, Kevin Mandia, January 2007.
- "What Pill Can I Take for Cyber Insecurity," *SC Magazine*, Kevin Mandia, July 2006.
- "Don't Hesitate to Call in the Professionals," *SC Magazine,* Kevin Mandia, October 2004.
- "We Must Beat These Automated Attackers," *SC Magazine*, Kevin Mandia, October 2004.
- *Incident Response: Performing Computer Forensics*, Kevin Mandia and Chris Prosise McGraw-Hill, copyright 2003.
- *Incident Response: Investigating Computer Crime,* Kevin Mandia and Chris Prosise, McGraw-Hill, copyright 2001.
- "Performing Live Forensic Analysis," *International Journal on Cyber Crime*, Kevin Mandia, January/March 2001, pages 2-6.
- "Conducting Corporate Intrusion Investigations," *International Journal on Cyber Crime*, Kevin Mandia, October/December 2000, pages 8-11.

HONORS AND AWARDS

- Selected as "Industry Professional of the Year" March, 2001 at the Techno-Security Conference.
- Certified Information Systems Security Professional (CISSP).

OTHER QUALIFICATIONS

- Currently has a Top Secret clearance.
- Was a Professorial Lecturer at the Graduate School level at Carnegie Mellon University.
- Was an adjunct professor of forensics at The George Washington University.
- Renowned speaker on computer forensics at some of the largest information security conferences, including: BlackHat, RSA Conference, Networld Interop, National Infragard Conference, GFIRST Conference, and many others.
- Computer forensics expert featured on CNN Talkback Live.
- Computer forensics expert featured on CNN Morning News Live.

EDUCATION

Master of Science in Forensic Science, The George Washington University, Washington D.C., 1995.
- Concentrations: Evidence handling, Federal Rules of Evidence, toxicology, pharmacology, anatomy, biological and physical aspects of the forensic sciences.
- Advisor: Walter F. Rowe

Bachelor of Science in Computer Science, Lafayette College, Easton, Pennsylvania, 1992.
- Concentrations: C language programming, database development, algorithms, assembly level programming, CPU engineering, and software engineering.

Attachment B

CASE EXPERIENCE FOR KEVIN MANDIA

Kevin Mandia specializes in electronic evidence discovery matters as well as responding to computer security incidents and security breaches. He has formally studied computer science, as well as forensics science, to blend technical acumen with proper evidence collection, review, and interpretation. He has trained hundreds of federal law enforcement from the Federal Bureau of Investigation and the United States Secret Service on investigating high-technology crimes such as theft of intellectual property, computer intrusions, and interpreting complex computer log files. His understanding of computer technology, computer networking, how data is stored and manipulated in computer systems, has been applied to over 50 investigations. Kevin is also a well recognized speaker in the area of computer forensics, incident response, and electronic evidence discovery.

Theft of Intellectual Property

Kevin has provided expert support for economic espionage investigations as well as theft of intellectual property cases. He has worked on cases that involved the comparison of registered, original computer programming source code with alleged stolen source code.

Unlawful and Unauthorized Access (Computer Intrusions)

Kevin has worked on dozens of investigations into unlawful or unauthorized access into computer systems on behalf of the U.S. Government as well as the victim organizations, insurance companies, or legal counsel. He has been published in the area of responding to computer security breaches, and has been an expert in federal court on these matters.

Kevin has been hired to provide opinions on many matters, including but not limited to the following:

- Whether financial databases were tampered with or not
- Whether personally identifiable information (PII) or intellectual property (IP) was compromised in a data security breach
- What a computer was primarily used for
- Whether a user possessed or disseminated a document or documents
- If a specific file was ever printed
- Whether a user wiped a drive or a file
- If web-based email accounts were used (e.g. Hotmail)
- If intentional deletion of materials occurred
- Whether or not external media devices were used
- What files were copied to the USB or remote media
- Whether a system was compromised or not

CRIMINAL CASE EXPERIENCE

UNITED STATES v. Bret McDanel, USDOJ, Southern District of California.
Kevin submitted numerous expert reports and testified as to the methods the defendant used to breach the computer security of the victim. Kevin also testified to provide a primer for understanding "hacking" and computer intrusions.

UNITED STATES v. Chad Grant, USDOJ, Southern District of California.
Kevin submitted numerous expert reports and testified as to the methods the defendant used to breach the computer security of the victim. Kevin also testified to provide a primer for understanding "hacking" and computer intrusions.

UNITED STATES v. Kai Xu and Hai Lin, USDOJ, District of New Jersey

Kevin submitted numerous expert reports and was the hired expert on the Economic Espionage case. The work involved the creation of expert reports that compared source code from the victim, Lucent Technologies, with source code found on the defendants systems.

UNITED STATES v. Walter A. Forbes and E. Kirk Shelton, USDOJ, District of New Jersey.
Kevin submitted several expert reports and provided opinions concerning the distribution of electronic documents.

UNITED STATES vs Alexey Ivanov, USDOJ, District of Connecticut.
Assisted on the expert reports and participated in proffer sessions.

UNITED STATES vs Vasily Gorchov, USDOJ, Western District of Washington.
Assisted the lead expert on analysis of data.

UNITED STATES v. Markus Lukawinsky, USDOJ, District of Connecticut.
Participated in the initial intrusion response. Provided intrusion and forensic analysis.

UNITED STATES v. Sami Omar Al-Hussayen, USDOJ, District of Idaho.
Assisted the lead expert on analysis of data.

UNITED STATES v. Robert Duronio, USDOJ, District of New Jersey.
Was the original expert hired. Assisted a co-worker who became the testifying expert.

UNITED STATES v.Michael Roman Afremov, USDOJ, District of Minnesota.
Participated as the computer forensics expert in reviewing financial databases to determine likelihood of tampering of the databases.

CIVIL CASE EXPERIENCE

DPL INC, THE DAYTON POWER AND LIGHT COMPANY, AND MVE INC (PLAINTIFF)
V.
PETER H. FORSTER, CAROLINE E. MUHLENKAMP, AND STEPHEN F. KOZIAR, JR., STATE OF OHIO, CASE NO: 04-5657
(DEFENDANT)

Involvement: Performed expert forensic analysis on behalf of the Plaintiffs, reviewing numerous drives to determine if electronic evidence was "wiped". Was deposed in December of 2006. Performed trial preparation. The case was settled in the midst of the trial in May 2007.

Libananco Holdings Co. Limited v. Republic of Turkey
ICSID Case No. ARB/06/8

Involvement: Kevin was hired to perform low-level analysis of floppy disks for evidence of timestamp manipulation. Testified at an International Tribunal.

Matthew Elvey and Gadgetwiz.com, Inc.
(PLAINTIFF)
V.
TD Ameritrade, Inc.
(DEFENDANT)
Case Number: 3:2007cv02852
Filed: May 31, 2007
Court: California Northern District Court
Office: San Francisco Office
Presiding Judge: Magistrate Judge Bernard Zimmerman

Involvement: Responded to a computer security data breach and provided technical and forensic support. Provided an opinion as to the likelihood that covered data was compromised by a computer breach.

EATON CORPORATION, ET AL.
(PLAINTIFF)
V.
JEFFRY D. FRISBY, ET AL
(DEFENDANT)
CIVIL ACTION NO.: 251-04-642CIV

Involvement: Worked with Special Master to produce evidence of theft of intellectual property.

QUEBECOR WORLD, INC., and QUEBECOR WORLD (USA), INC.,
(PLAINTIFF)
V.
R.R. DONNELLEY & SONS COMPANY, JAMES ("KIP") ALEXANDER, JOSEPH GENTILE, JOHN KINGSTON, ROBERT ROMPALA, and CHARLES SCHWERMAN,
(DEFENDANTS)

Involvement: Performed full forensic analysis of more than 5 systems to determine whether prior employees conducted theft of intellectual property.

MICHAEL A. MURRAY (PLAINTIFF)

V.
MERRILL LYNCH, PIERCE, FENNER & SMITH INCORPORATED AND ROBERT EWING IV, AND RANDY KIRBY
(DEFENDANT)
NASD DISPUTE RESOLUTION CASE NUMBER: 03-02346, M.L. FILE NUMBER: 2003000428

Involvement: Performed in-depth forensic analysis of the Plaintiff's system to determine prior knowledge of specific stocks/financial expertise.

LOCKHEED MARTIN CORPORATION,
(PLAINTIFF)
V.
THE BOEING COMPANY, MCDONNELL DOUGLAS CORPORATION, BOEING LAUNCH SERVICES, INC., WILLIAM ERSKINE, KENNETH BRANCH, AND
LARRY SATCHELL
(DEFENDANTS)
CASE NO. 6:03 CV 796 ORL 28 KRS

Involvement: Produced numerous electronic discovery requests, written opinions on collection requirements, and a declaration. Provided electronic evidence discovery services.

ELOUISE PEPION COBELL, ET AL.
PLAINTIFFS
V.
GALE A. NORTON, SECRETARY OF THE INTERIOR, ET AL.,
DEFENDANTS
NO. CIV.A.96-1285 RCL.

Involvement: Assisted Special Master John Bickerman on the case that took the Department of Interior Bureau of Indian Affairs of the Internet. This case involved our assessment of the DOI computer security practices and advised the Special Master on IT security issues.

MEDTRONICS
(PLAINTIFF)
V
MICHELSON
(DEFENDANT)

Involvement: Wrote numerous declarations concerning electronic evidence discovery and collection requirements. Advised special master on spoliation issues and likelihood of recovering deleted information.