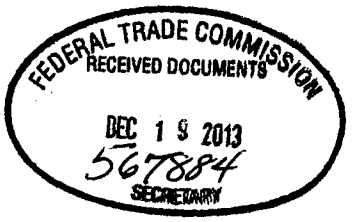
ORIGINAL



UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION
OFFICE OF ADMINISTRATIVE LAW JUDGES

In the Matter of	)	**PUBLIC**
LabMD, Inc., a corporation, Respondent.	)	Docket No. 9357

OPPOSITION TO MOTIONS TO QUASH AND FOR PROTECTIVE ORDER REGARDING SUBPOENAS SERVED ON SCOTT MOULTON AND FORENSIC STRATEGY SERVICES, LLC

INTRODUCTION

Complaint Counsel submits this opposition to the Motions to Quash and for Protective Order filed by LabMD, Scott Moulton, and Forensic Strategy Services, LLC ("Forensic") regarding Complaint Counsel's subpoenas to Scott Moulton and Forensic. Because the motions of LabMD, Inc. ("LabMD"), Moulton, and Forensic present largely identical arguments, Complaint Counsel hereby submits this consolidated response for the Court's convenience.

This Court should deny the Motions to Quash and for Protective Order because they seek to shield from discovery facts that bear on the allegations of the Complaint, the proposed relief, and LabMD's anticipated defenses. To the extent that any attorney work product immunity from discovery may apply, neither Respondent nor Moulton nor Forensic have made the requisite showing by producing a privilege log. Relatedly, Complaint Counsel is entitled to discovery of the facts underlying and asserted in a public affidavit used by LabMD in litigation.

Further, LabMD's and Moulton's respective motions are untimely. Finally, a confidentiality provision in a private contract – that in any event excludes information made

public by LabMD – is not a legitimate basis for resisting information sought in a government subpoena.

BACKGROUND

The Complaint alleges that LabMD engaged in unfair practices in violation of Section 5 of the FTC Act by failing to take reasonable and appropriate measures to prevent unauthorized access to consumers' personal information. Compl. ¶¶ 6-11, 17-21. One of the results of LabMD's failures is that a LabMD file containing the sensitive personal information of approximately 9,300 consumers ("the P2P insurance aging file") was shared to a public peer-to-peer ("P2P") file sharing network without being detected by LabMD. *Id.* ¶¶ 10(g), 17-20.

As a preliminary matter, LabMD incorrectly assumes that this action relates only to LabMD's exposure of sensitive consumer data over P2P networks. In fact, the Complaint alleges that LabMD's overall data security practices were woefully inadequate, creating potential exposure of consumer data on many fronts. See Compl. ¶ 10 (outlining several deficiencies in LabMD's data security practices). The exposure of names, dates of birth, Social Security numbers, codes for lab tests conducted, health insurance company names, addresses, and policy numbers to the public over the P2P network is a prime example and a devastating consequence of LabMD's lax data security.

In May 2008, Tiversa, Inc. ("Tiversa") informed LabMD that the file LabMD exposed was available on a public file sharing network. *Id.* ¶ 17. LabMD subsequently filed suit in Georgia state court against Tiversa, asserting a variety of claims related to Tiversa obtaining the P2P insurance aging file. *LabMD, Inc. v. Tiversa, Inc.*, No. 11-cv-04044 (N.D. Ga. Nov. 23, 2011). The case was removed to federal court, and Tiversa filed a motion to dismiss.

In LabMD's response to Tiversa's motion to dismiss, LabMD attached an affidavit from Scott Moulton, an IT provider it retained. *See* Affidavit of Scott A. Moulton, *LabMD, Inc. v. Tiversa, Inc.*, No. 11-cv-04044 (N.D. Ga. Jan. 13, 2012), ECF No. 16-1 (attached as Exhibit A). Moulton is the President of and Lead Certified Computer Forensic Specialist for Forensic. *See id.* Moulton's affidavit, as outlined below, includes facts that bear directly on the Complaint's allegations, the proposed relief, and LabMD's anticipated defenses, including: the P2P insurance aging file, which the affidavit refers to as the "May 13 file"; LabMD's contention that Tiversa stole the P2P insurance aging file by opening a physical TCP/IP connection on LabMD's computer[1]; and the availability of the P2P insurance aging file on computers outside of LabMD.[2] *Id.* ¶¶ 5-15.

Indeed, as part of its defense in this matter, LabMD has asserted that the P2P insurance aging file was stolen from LabMD through a hack of its network. *See, e.g.*, Transcript of Initial Scheduling Conference at 24, Statement of Reed Rubinstein, Cousel for LabMD, Inc., In the Matter of LabMD, Inc., FTC Docket No. 9357 (Sept. 25, 2013) ("And actually, I would like to if

---

[1] Complaint Counsel intends to show that LabMD is simply wrong that Tiversa accessed LabMD's network to obtain the insurance aging file. Instead, the evidence will show that Tiversa obtained the file not from LabMD but from the computers of parties not related to LabMD.

[2] Moulton's work for LabMD also is chronicled in *The Devil Inside the Beltway*, a book published by LabMD's CEO, Michael Daugherty. Michael J. Daugherty, *THE DEVIL INSIDE THE BELTWAY* 329, 332-33 (Broadland Press 2013).

I could, just take issue with the file that triggered this investigation was not shared; it was stolen. A company called Tiversa . . . .").[3]

Based on Moulton's affidavit in the Tiversa case, Complaint Counsel issued subpoenas to Moulton and Forensic on October 24, 2013.[4] Moulton and Forensic did not move to quash Complaint Counsel's subpoenas in the time period prescribed by Rule 3.34(c), which elapsed on November 6, 2013. 16 C.F.R. § 3.34(c).

On November 5, 2013, LabMD filed a Motion for a Protective Order that sought to prevent Complaint Counsel from engaging in third party discovery, specifically naming Moulton and Forensic. *See* Respondent LabMD, Inc.'s Motion for a Protective Order at 2 n.1, In the Matter of LabMD, Inc., Docket No. 9357 (Nov. 5, 2013). At no point did LabMD raise in its November 5, 2013 Motion any of the arguments it now asserts with respect to Moulton and Forensic. *Id.*

On November 21, 2013, the deadline for Moulton and Forensic to produce documents, Complaint Counsel received a letter from Moulton, dated November 19, 2013, outlining objections to Complaint Counsel's document subpoenas.[5] *See* Letter from Scott Moulton, Forensic Strategy Services, LLC to Matthew Smith, Paralegal, Federal Trade Commission (Nov. 19, 2013) (attached as Exhibit B) ("November 19 letter").

---

[3] LabMD further put the subject of Moulton's affidavit at issue in this matter by questioning Robert Boback, the CEO of Tiversa, in a November 2013 deposition regarding Tiversa's acquisition of the P2P insurance aging file.

[4] LabMD (Resp. Motion at 1) and Forensic's (Forensic Motion at 1) assertion that Complaint Counsel served a deposition subpoena on Forensic is mistaken. It served a deposition subpoena on Moulton, and document subpoenas on Moulton and Forensic.

[5] At that time, Moulton and Forensic were not represented by counsel in this matter.

Upon receipt of the November 19 letter, Complaint Counsel called Moulton. During this call, Moulton agreed to be deposed on February 6, 2014 but stated that he would refuse to answer any questions about LabMD, citing attorney work product. Complaint Counsel re-served Moulton on November 27, 2013 for his February 6, 2014 deposition.

On December 6, 2013, Complaint Counsel spoke by phone with LabMD's counsel regarding the subpoenas to Moulton and Forensic. LabMD's counsel requested that Complaint Counsel withdraw its subpoenas and stated that it would move to quash the subpoenas and seek a protective order if Complaint Counsel did not withdraw them.

On December 9, 2013, Complaint Counsel spoke with counsel retained by Moulton and Forensic, who likewise requested that Complaint Counsel withdraw its subpoenas and indicated that it otherwise would move to quash the subpoenas and seek a protective order. At no point during the December 6, 2013 or December 9, 2013 calls did LabMD's counsel or Moulton and Forensic's counsel state that they considered Moulton an expert consultant; nor did they reveal LabMD's intentions about not designating Moulton as an expert in this matter. Although their motions invoke the attorney work product doctrine, Moulton and Forensic have not to date provided Complaint Counsel with a privilege log, as requested in the document subpoenas and as required under Rule 3.38(A). 16 C.F.R. § 3.38A.

ARGUMENT

I. COMPLAINT COUNSEL'S SUBPOENAS TO MOULTON AND FORENSIC ARE REASONABLY EXPECTED TO YIELD INFORMATION RELEVANT TO ALLEGATIONS OF THE COMPLAINT, PROPOSED RELIEF, OR DEFENSES IN THIS ACTION

Complaint Counsel's subpoenas seek discovery "reasonably expected to yield information relevant to the allegations of the complaint, to the proposed relief, or to the defenses

of any respondent." 16 C.F.R. § 3.31(c)(1). The facts Moulton asserts in his publicly filed sworn affidavit and that also appear in a published book relate directly to the Commission's allegations. These facts also were put at issue by LabMD in this litigation and therefore relate to LabMD's defenses. *See, e.g.,* Transcript of Initial Scheduling Conference at 24, Statement of Reed Rubinstein (Sept. 25, 2013).

For example, Moulton states in his affidavit that he examined the computer file Tiversa presented to LabMD and the file has a unique SHA-1 value.[6] *See* Affidavit of Scott A. Moulton ¶ 13. Moulton also states that he has not found any evidence that the file Tiversa presented to LabMD exists on any computer other than the LabMD computer where the file was saved. *Id.* ¶ 15. These facts are directly relevant to the Complaint's allegations regarding the reasonableness of LabMD's data security practices and the P2P file sharing incident, as well as LabMD's defenses about the widespread availability of the insurance aging file, Compl. ¶¶ 10, 13-20. Therefore, LabMD's contention that the documents and testimony sought from Moulton, particularly the facts in Moulton's affidavit and the facts supporting it, lack relevance to this action is without merit.

LabMD engaged Moulton and his company to examine the insurance aging file, analyze its metadata, and search P2P networks for the file. LabMD then publicly disclosed Moulton's work and the results of it in a court-filed affidavit and a publicly available book. Having done so, LabMD cannot now seek to hide Moulton's work, the methods and techniques he used, and the results of his investigation. Each is highly relevant to the claims at issue in this action, as well as defenses raised by LabMD in this action.

---

[6] An SHA-1 value is a unique signature associated with the file.

II. LABMD WAIVED THE ATTORNEY WORK PRODUCT DOCTRINE AS TO MOULTON'S AFFIDAVIT AND THE FACTS UNDERLYING IT AND CANNOT HIDE BY LABELING MOULTON AN EXPERT CONSULTANT

In evaluating LabMD's work product claim,[7] this Court should find that LabMD waived it with respect to Moulton's affidavit and the facts underyling it.[8] Facts put forth by LabMD to support its defense are included in Moulton's public affidavit and disclosed in Daugherty's book. Because LabMD publicly disclosed Moulton's affidavit and has squarely raised as a defense *in this litigation* the circumstances under which Tiversa came into possession of the P2P insurance aging file, it is appropriate for Complaint Counsel to seek discovery on these issues. *See* 8 CHARLES ALAN WRIGHT ET AL., Federal Practice and Procedure, §§ 2016.4, 2016.6 (3d ed. Apr. 2013) (explaining work product protection is waived when holder of protection puts protected material at issue).

LabMD (as well as Moulton and Forensic) cannot now attempt to frustrate discovery by labeling Moulton an expert consultant. Complaint Counsel should be permitted to obtain documents that Moulton relied upon when preparing his affidavit as well as question Moulton about the facts in his affidavit and the facts underyling it. Further, like Moulton and Forensic, LabMD has not to date provided Complaint Counsel with a privilege log or even a description of the documents subject to the protection invoked in its motion, and the Court should order one to

---

[7] It is well-established that to the extent that the attorney work product may be applicable here, it does not belong to Moulton and Forensic. *See In re OSF Healthcare Sys.*, No. 9349, 2012 WL 1355596, at *1 n.2 (noting that work product does not belong to third party consultant retained by Respondents but to Respondents directly); *In re Grand Jury Subpoenas*, 561 F.3d 408, 411 (5th Cir. 2009) (holding that attorney work product belongs to attorney and client). On this basis, this Court should disregard Moulton and Forensic's invocation of attorney work product.

[8] Moulton and Forensic could not be subjected to liability to LabMD for violating the work product doctrine when LabMD waived any such protection.

be produced. To the extent attorney work product may be applicable, Complaint Counsel should be permitted to assess the bases of such claims with a log required by Rule 3.38A, and to test this claim by examining Moulton.

III. MOTIONS TO QUASH AND MOTION FOR PROTECTIVE ORDER ARE NOT TIMELY

The Motions of Moulton and LabMD to quash the deposition subpoena served on Moulton are not timely. Under Rule 3.34(c), a motion to quash "shall be filed within the earlier of 10 days after service thereof or the time for compliance therewith." 16 C.F.R. § 3.34(c). Complaint Counsel effected service on Moulton's deposition subpoena on October 25, 2013, meaning that the 10-day window to file a motion to quash has long closed.

Further, LabMD has been in possession of Complaint Counsel's subpoenas since October 24, 2013. LabMD could have raised any of the arguments it is now making in its November 5, 2013 Motion for a Protective Order seeking to prevent the discovery of Moulton and Forensic but elected not to do so. *See* Respondent LabMD, Inc.'s Motion for a Protective Order, In the Matter of LabMD, Inc. Docket No. 9357 at 2, n.1 (Nov. 5, 2013). Now that this Court has ruled that the third party discovery of Moulton and Forensic should proceed, LabMD should not get another bite at the apple by raising arguments it could have previously raised.

IV. A CONTRACTUAL CONFIDENTIALITY PROVISION IS NOT A DEFENSE

Moulton and Forensic also erroneously assert that a protective order is necessary to prevent them from breaching the confidentiality provision in Forensic's contract with LabMD. This claim is without merit, as a private contractual confidentiality provision must yield to a government subpoena. *See, e.g., E.E.O.C. v. Severn Trent Svcs., Inc.*, 358 F.3d 438, 442 (7th

Cir. 2004) (private contracts cannot trump government subpoenas). Similary, private confidentiality agreements cannot serve as a bar to discovery, especially when balanced against the need for discovery in litigation. *See, e.g., Zoom Imaging, L.P. v. St. Luke's Hosp. & Health Network*, 513 F.Supp.2d 411, 417 (E.D. Pa. 2007) (holding private confidentiality agreement does not protect material from discovery).

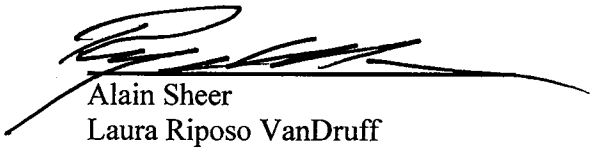
Alternatively, the confidentiality provision in the contract between Forensic and LabMD contains an exception for publicly disclosed information (attached as Exhibit C). LabMD's public disclosure in an affidavit and book of the nature of Moulton and Forensic's work and their findings therefore vitiates any contractual requirement of Moulton and Forensic regarding disclosure of this information.

CONCLUSION

For the foregoing reasons, the Court should deny the Motions to Quash and for Protective Order regarding Scott Moulton and Forensic Strategy Services, LLC.

Dated: December 19, 2013

Respectfully submitted,



Alain Sheer
Laura Riposo VanDruff
Megan Cox
Margaret Lassack
Ryan Mehm
John Krebs

Federal Trade Commission
600 Pennsylvania Ave., NW
Room NJ-8100
Washington, DC 20580
Telephone: (202) 326-2918 – Mehm
Facsimile: (202) 326-3062
Electronic mail: rmehm@ftc.gov

Complaint Counsel

CERTIFICATE OF SERVICE

I hereby certify that on December 19, 2013, I filed the foregoing document electronically through the Office of the Secretary's FTC E-filing system.

I also certify that I caused a copy of the foregoing document to be delivered *via* electronic mail and by hand to:

The Honorable D. Michael Chappell
Chief Administrative Law Judge
Federal Trade Commission
600 Pennsylvania Avenue, NW, Room H-110
Washington, DC 20580

I further certify that I caused a copy of the foregoing document to be served *via* electronic mail and *via* Federal Express to:

Elizabeth G. Howard
Barrickman, Allred & Young, LLC
5775 Glenridge Drive
Building E, Suite 100
Atlanta, GA 30328
egh@bayatl.com

I further certify that I caused a copy of the foregoing document to be served *via* electronic mail to:

Michael D. Pepson
Cause of Action
1919 Pennsylvania Avenue, NW, Suite 650
Washington, DC 20006
michael.pepson@causeofaction.org
lorinda.harris@causeofaction.org
hallee.morgan@causeofaction.org

Reed Rubinstein
William Sherman, II
Dinsmore & Shohl, LLP
801 Pennsylvania Avenue, NW, Suite 610
Washington, DC 20004
reed.rubinstein@dinsmore.com

william.sherman@dinsmore.com
Counsel for Respondent LabMD, Inc.

CERTIFICATE FOR ELECTRONIC FILING

I certify that the electronic copy sent to the Secretary of the Commission is a true and correct copy of the paper original and that I possess a paper original of the signed document that is available for review by the parties and the adjudicator.

December 19, 2013

By: 

Ryan Mehm
Federal Trade Commission
Bureau of Consumer Protection

Exhibit A

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

LABMD, INC.,	)	
	)	
Plaintiff,	)	
	)	**Civil Action**
v.	)	
	)	**File No. 1:11-cv-04044-JOF**
TIVERSA, INC., TRUSTEES OF DARTMOUTH COLLEGE, M. ERIC JOHNSON,	)	
	)	
Defendants.	)	

AFFIDAVIT OF SCOTT A. MOULTON

Personally appeared before the undersigned officer duly authorized to administer oaths, Scott A. Moulton, who after being duly sworn, deposes as follows:

1.

I am over 18 years of age, I am under no disability, and I am competent to give this affidavit. I give this affidavit of my own free will, and for use in the above-styled case, and for any other lawful purpose. The contents of this affidavit are based on my personal knowledge and my professional expertise.

2.

I am President of and Lead Certified Computer Forensic Specialist for Forensic Strategy Services, LLC. Since becoming involved in computer forensics,

I have developed extensive expertise in this area as well as provide training for police agencies all over the world on the specifics of forensics. I am a Certified Computer Forensic Specialist and have been in the industry of computer forensics for eleven years. I have been certified as a computer forensic specialist for nine years. My Curriculum Vitae is attached hereto as Exhibit "A."

3.

In order to discuss forensics and perform the duties of investigations and surveillance, the State of Georgia requires me to hold a Private Investigators License. I am a licensed Private Investigator in the State of Georgia as required.

4.

I have reviewed the Complaint and supporting exhibits filed in the above-referenced action. After reviewing Exhibit B to the Complaint, I learned that Defendants Tiversa and M. Eric Johnson, with Defendant Dartmouth's knowledge and consent, searched peer-to-peer ("P2P") networks and randomly gathered a sample of shared files related to health care and health care institutions. Defendant Tiversa's servers and software allowed Defendant Dartmouth and Defendant Johnson to sample for files in the four most popular P2P networks (each of which supports the most popular clients) including Gnutella, Aries and e-donkey. *See* Exhibit B to complaint, p.8.

5.

Through my work as a private investigator, I have examined P2P networks, including the Gnutella network. In my examination of the Gnutella P2P file sharing network, I have learned that computers on the Gnutella P2P network have software installed on them that facilitate the trading of computer files including images and videos. The software, when installed, allows the user to search for the pictures, movies, and other digital files by entering text as search terms. Some names of the software used include, but are not limited to, BearShare, LimeWire, Shareaza, Morpheus, Gnucleus, Phex and other software clients. Those software programs interface with the Gnutella Network and are called Gnutelliums and are simply user interfaces with the underlying network of other users.

6.

When a user makes a search request on the P2P Gnutella network, the search goes through an Ultra-peer and checks the listings on the computers connected to the Gnutella network. When a file is found that the user wants to download and a request for the file is made, the file comes directly from the Internet Protocol ("IP") address of the computer where the file is physically located because Ultra-peers only have the file listing and not the actual file.

7.

When a user seeks to download a file from the P2P Gnutella network, the P2P Gnutella network software program opens a Transmission Control Protocol / Internet Protocol ("TCP/IP") port at the site where the file is located.

8.

TCP/IP is a way of connecting to a host computer. In order to connect to a host computer, the computer seeking access to the host computer sends a command to the host computer to open a port at the host site and to transfer data from the host site.

9.

Opening a TCP/IP port to connect to a host computer at another location is the same as physically being at the host site to take action on the file.

10.

When Defendants Tiversa, Mr. Johnson and Dartmouth College searched for the May 13 File, they opened a physical TCP/IP connection on LabMD's computer located in the State of Georgia.

11.

Every computer file being shared on the Gnutella P2P network has a unique file signature called a Secure Hash Algorithm (SHA) version 1 ("SHA 1").

SHA 1 was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA). A SHA-1 value can be likened (in layman terms) to DNA. It is a mathematical fingerprint of a computer file that will remain the same for an unchanged file no matter where the file is found or on which computer the file is located. Changing the file name will not make a change to the actual digital file, nor will sending or trading the same file across the Internet change the digital signature.

12.

The Gnutella P2P network software clients that connect and share files calculate the SHA-1 values of the files in the user's shared folder upon start up of the software. The Gnutella Client Software makes the file names and those values available on the network.

13.

I have examined the computer file presented to LabMD from Defendant Tiversa on May 13, 2008 ("May 13 File"). The May 13 File has a unique SHA-1 value.

14.

If LabMD deleted the May 13 File, also known as the 1,718 File in LabMD's Complaint, from its computers, a person searching for the file will be unable to

locate a copy of the file because the P2P Gnutella network searches for files based upon the SHA-1 value.

15.

In connection with my forensic work on this matter, I have not found any evidence that the May 13 File exists on any other computer other than the LabMD computer where the file was saved.

16.

I hold all the foregoing opinions to a reasonable degree of certainty. All fees paid for my services are in no way contingent upon the results of my examination and report. I have no financial interest in the outcome of this action.

FURTHER AFFIANT SAITH NOT, this 12 day of Jan, 2012.

SCOTT A. MOULTON

Sworn and subscribed before me
This 12 day of Jan, 2012

NOTARY PUBLIC
My commission expires:
May 12, 2014

PATRICIA GILBRETH
NOTARY PUBLIC
FORSYTH COUNTY GEORGIA
My Commission Expires
May 12, 2014

Scott A. Moulton
Forensic Strategy Services, LLC.
601B Industrial Court
Woodstock, Ga 30189
Email: smoulton@ForensicStrategy.com

Phone: 770-926-5588
Fax: 770-926-7089
Cell: 770-402-0191
Web: www.ForensicStrategy.com

Scott A. Moulton

Mr. Scott Moulton, CCFS: Certified Computer Forensic Specialist

Mr. Moulton is president of Forensics Strategy Services, LLC. and began the company in 2000. Mr. Moulton is skilled in the areas of data recovery and system recovery including rebuilding Exchange servers and has spent the last seven years focusing on computer forensics.

Positions & Skills

President, Forensic Strategy Services, LLC. Woodstock, GA (2000-Present)
Forensic Data Recovery Litigation Support Expert, Private Detective

- Handle complete forensic data collection and preparation of evidence where a personal computer contains data that may be useful in a legal case
- Developed and implemented a methodology when handling equipment and hard drives involved in forensic data recovery while maintaining the chain of custody
- Authored and published in magazines on the topic of computer forensics
- Skilled in rebuilding hard drives and forensic preservation of damaged drives
- Speaker on topic of data recovery and rebuilding hard drives and forensic topics
- Identification of internal security issues
- Georgia Employee Licensed Private Detective

President, Network Installation Computer Services, Inc. Woodstock, GA (1993-Present)
Senior Computer System Specialist

- Technical Support for Data Recovery and Backup Protection
- Responsible for informing other staff of new methods for security and recovery
- Primary lead technician and system engineer

Partner, Docupak Technologies, Inc. Kennesaw, GA (2001-Present)
Forensic Developer

- This team has a staff of web developers that has done projects for
- Georgia Pacific, Six Flags, etc.
- When a case that involves custom code or a specialized case that requires
- someone with experience in development, my status allows me to redirect
- employees from this company to help in forensic cases

Time Plus, Inc. Marietta, GA (June 1990-1993)
Networking and Accounting Support Consultant

- Responsible for building and support of Novell Networks
- Responsible for support for all customer accounting servers using Solomon III/IV
- Development and code testing on project to Lockheed Martin

EXHIBIT - A

Scott A. Moulton
Forensic Strategy Services, LLC.
601B Industrial Court
Woodstock, Ga 30189
Email: smoulton@ForensicStrategy.com

Phone: 770-926-5588
Fax: 770-926-7089
Cell: 770-402-0191
Web: www.ForensicStrategy.com

Experience with Software and Hardware:

- Forensic Imaging Specifications
- Experienced with Encase 4, 5 and 6
- Access Data FTK and Registry Tools
- Rebuilding Raid Arrays
- Expert in Data Recovery and Data Recovery Software, Runtime Software
- Expert in Rebuilding damaged Hard Drives
- Internal Windows System Recovery Formats
- Evidence Eliminator Software
- Hardware Write Blockers for Forensic Images with Tamper Resistant Processes
- CD Manufacturing and Data Recovery from CD's/DVD's
- RAID Array Systems and Recovery of Crashed RAID Systems
- Indexing and Search Software
- Most Hard Drives ever made, including assembly and disassembly of inner components
- Exchange Server, All Email Servers, Lotus Notes Email Servers
- Novell Operating Systems
- Microsoft Products Including but not limited to:
  - Microsoft Operating Systems
    - Windows 2003 Server
    - Windows 2003 Advanced Server
    - Windows NT Server
    - Exchange Server 2000 & 2003
  - ISA and Proxy Server and firewalls
  - Terminal Server and Advanced Terminal Server
  - Microsoft applications
- Internet and Web Applications
- Palm and Pocket PC System including the Data Recovery of both.
- Recovery of Photos and Pictures from Digital Camera and Digital Memory Sticks
- Recovery of all Firewire and USB Equipment
- Hardware and Software Sniffers, including Wireless
- Custom Written Tracking Systems and Monitoring Systems
- Firewalls both Hardware and Software
- Routers including Cisco, Ascend, Lucent
- Remote Application Software Including:
  - VPN, LAN, WAN
  - Web Sites
  - Web Applications
  - E-Commerce
- Windows Based Security Systems

Memberships and Clubs:

- Member of the Certified Fraud Examiners
- Woodstock Powercore Team Coordinator
- Toastmasters Cobb Micro Enterprises Kennesaw
- Interz0ne, LLC. Seminar Speaker
- GrayArea, LLC. Training Leader
- Defcon 404 Local Chapter
- Attending Defcon Las Vegas
- Electronic Frontier Foundation Member
- Licensed Encase 4 & 5 Investigator
- Licensed FTK Investigator

Scott A. Moulton
Forensic Strategy Services, LLC.
601B Industrial Court
Woodstock, Ga 30189
Email: smoulton@ForensicStrategy.com

Phone: 770-926-5588
Fax: 770-926-7089
Cell: 770-402-0191
Web: www.ForensicStrategy.com

Certifications

- CCFS: Certified Computer Forensic Specialist
- CCFT: Certified Computer Forensic Technician
- Georgia Employee Licensed Private Detective
- Aptec – IOUC System Programmer and Developer Certified
- Microsoft Developer Network
- Microsoft Business Partner
- Lotus Business Partner
- Lotus Notes Developer
- Solomon III Accounting Server
- Solomon IV Accounting Server
- Solomon IV Accounting System Developer
- Novell Certified Network Administrator
- Trend Micro Security Solution Partner
- Dell Solution Provider

Education & Training

1993 – Present **Training Events and Courses**

- Taught Several Training Seminars on Computer Forensics, Computer Technology and Terminology, Application Usage and Presentation Formats
- Taught Forensics 101 Class to EarthLink's Fraud Department
- Completed Standard Computer Forensics & Electronic Discovery Training Course
- Completed Advanced Computer Forensics & Electronic Discovery Training Course
- Completed Lotus Notes Training Course
- Attended Training at Southeastern Cybercrime Summit.
- Forensic Training from Business Intelligence Associates
- "The Certified Fraud Examiner in Court"
- "Trends in Fraud Litigation"
- "Ethical Lessons for Financial Professionals"
- "Data Presentation" for Court sponsored by Certified Fraud Examiners
- "Best Practices for Data Protection and Recovery" by Winternals
- "Using Data Analysis Techniques to Find Fraud"
- "Data Retrieval and Data Protection" by David Benton, Georgia Bureau of Investigation

Attending:

1986 – 1991 Southern College of Technology Marietta, Ga
Computer Science Major

- Campus Radio Announcer
- Computer consultant

1982 – 1986 Benedictine Military Academy Savannah, Ga
College Preparatory With Distinction

- Savannah Stamp and Philatelic Society

Accomplishments

- Written and published in magazines on the topic of computer forensics
- Rebuilt hard drives and head assemblies successfully
- Attend All Certified Fraud Examiner meetings possible
- Participate in ACT Training Program as an Instructor for Internships
- Developed "Proof of Concept" Forensic Data Slurping Application
- Worked on application for F-22 for Lockheed under TimePlus
- Responsible for Reporting several bugs and fixes to Encase and Access Data teams

Exhibit B