UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

PAUL D. CEGLIA, Plaintiff, v. MARK ELLIOT ZUCKERBERG and FACEBOOK, INC., Defendants.	Civil Action No. 1:10-cv-00569-RJA **DECLARATION OF MICHAEL F. MCGOWAN IN SUPPORT OF DEFENDANTS' MOTION FOR EXPEDITED DISCOVERY**

I, Michael F. McGowan, declare and state as follows:

Introduction

1. Stroz Friedberg, LLC ("Stroz Friedberg") has been retained by Gibson, Dunn & Crutcher, LLP ("Gibson Dunn"), on behalf of its clients Mark Zuckerberg and Facebook, Inc. ("Facebook"), in the above-styled case to provide consulting and electronic discovery services and to conduct digital forensic examinations of various media. This declaration is executed by Michael F. McGowan, a Director of Digital Forensics at Stroz Friedberg. I have helped lead the development of Stroz Friedberg's expertise in detecting backdating and forgeries of electronic documents.

2. I have been informed by Gibson Dunn that Paul Ceglia claims to possess a contract between himself and Mr. Zuckerberg regarding "The Face Book" that Mr. Ceglia prepared and saved on his computer (the "Purported Contract"), as well as email messages between Mr. Ceglia and Mr. Zuckerberg regarding the ownership of "The Face Book" (the "Purported Emails"). I also have been informed that Mr. Zuckerberg and Facebook maintain that these documents are fabricated in whole or in part. I further have been informed that Mr. Ceglia claims to have recently discovered the existence of the Purported Emails on computers in his parents' home.

3. As set forth below, Stroz Friedberg has extensive experience and is a leading expert in assessments as to whether electronic documents have been backdated, forged, or altered. As explained below, to best make such assessments, Stroz Friedberg needs to inspect: (a) all native electronic versions of the Purported Contract and the Purported Emails; and (b) every available computer or piece of external media on which the electronic documents in question were created, viewed, saved, or modified. As explained below, there can be substantial information in the native electronic versions of the files in question that bear on their authenticity. Producing printouts, Adobe Acrobat .pdf files, or other similar non-native copies of the documents do not give a digital forensic examiner comparable access to the critical existing evidence bearing on authenticity.

4. In addition, as explained below, evidence relating to authenticity can be extracted from many locations on any computers on which the documents in question were created, saved, viewed, or modified. These locations include the computer system, application, and security logs; the unallocated space of the computers from which deleted files or file fragments may be recovered; the portion of the hard drives that stores the dates and times that files were created, last accessed, and modified; and the files that show what documents recently were accessed.

5. Accordingly, this declaration is in support of Gibson Dunn's motion for expedited discovery requiring Mr. Ceglia to produce for forensic preservation and unfettered digital forensic analysis: (a) all native electronic versions of the Purported Contract and the Purported Emails; and (b) all computers and electronic media within Mr. Ceglia's possession, custody, or control, including the computers found at his parents' house on which Mr. Ceglia claims to have found the copies of the Purported Emails on which he now relies. As further described below, creating forensically-sound copies of this native data and these computers and electronic media is critical to performing an assessment of whether the Purported Contract and the Purported Emails are legitimate or the product of fraud.

Qualifications in E-Forgery Matters

6. I have gained expertise through experience, research, and training in detecting e-forgeries. I have conducted digital forensic examinations of multiple computers, external hard drives, and other digital media in both routine cases and cases in which many millions of dollars or people's freedom have hinged on the authenticity of proffered electronic documents. In many cases, I have been able to find critical evidence that bore on the authenticity of the electronic documents and, in a majority of the cases, that evidence has resolved the matter.

7. I am a Director of Digital Forensics at Stroz Friedberg. I co-manage Stroz Friedberg's technical operations in the areas of digital forensics and cyber-crime response. I have conducted hundreds of digital forensic examinations and data acquisitions from various media types, including laptop and desktop computers, servers, and mobile devices. I also have been the lead digital forensic examiner on most of the firm's significant e-forgery investigations. I have provided trial and hearing testimony on a number of occasions and have been admitted as an expert in digital forensics in federal and state court, including on behalf of the United States Department of Justice in connection with one of the Enron Task Force prosecutions. A copy of my C.V. is attached to this declaration as Exhibit A.

8. On this matter, I worked under the direction and supervision of Eric M. Friedberg. Mr. Friedberg is Co-President of Stroz Friedberg. He has participated in and supervised hundreds of digital forensics examinations over his past eleven years with Stroz Friedberg, both in the context of litigation-related disputes and responses to cyber-crime. He has participated in and supervised almost all of the firm's e-forgery matters, including those on which I was the lead digital forensics examiner. These e-forgery matters have involved disputes over the authenticity of contracts, e-mails, movie scripts, and memoranda. He has published an article and lectured on

e-forgery. Prior to joining Stroz Friedberg, Mr. Friedberg was an Assistant United States Attorney with the United States Attorney's Office for the Eastern District of New York from 1989 to 2000. Mr. Friedberg acted at various times as the Office's Chief of Narcotics and the district's lead cyber-crime prosecutor. A copy of Mr. Friedberg's C.V. is attached to this declaration as Exhibit B.

Conducting the Authenticity Analysis

A. Information Available from the Native Electronic Files

9. In an authenticity case, it is critically important for a digital forensic expert to have available for examination more than the paper printouts or images (.pdf or .tiff files) of the documents. A digital forensic examiner should have full access to every available version of the "native" electronic files at issue, meaning the format in which the file was originally created. For example, email stored by a user using Microsoft Outlook should be produced in Outlook format, normally in a file called a ".pst file". As another example, Microsoft Word documents should be produced as Word documents (.doc or .docx files). If a Word document has been rendered as a .pdf file, then the Word version and the .pdf version should be produced.

10. Native electronic documents contain certain data about the creation and use of the documents. This data is called "embedded metadata" and can include information about the date the document was created, last accessed, modified, and printed; the author of the document; the name of the user who last opened the document; the date an email was sent or modified; and other information. This data can be critical in authenticating a document, as anomalies in this metadata can constitute clear proof of backdating or fraudulent editing.

11. Native emails also contain many embedded metadata attributes that are useful in determining authenticity. Some of that embedded metadata is immediately visible on the face of

an email, such as the sender of the email, the recipients of the email, the date and time the email was sent or received, and the subject of the email. However, a digital forensic examination of an email produced in native format can reveal other useful embedded metadata, such as the Internet headers. When an email is transmitted across the Internet from the sender to the recipient, each server that is used in the transmission affixes the date and time at which the email was received by the server to the email's Internet headers metadata. Anomalies in the Internet headers can readily reveal backdating and fraud. An analysis of email Internet headers, including the date and time stamping, is critical in a case such as this where Mr. Ceglia is claiming that key emails were exchanged over the Internet between him and Mr. Zuckerberg in or around 2003 and 2004.

12. Native files also can include other non-visible data that can bear on authenticity, such as Track Changes information that reveal a document's editing history or recent deletions from the document that can be forensically reconstructed. Such information is necessary to fully understand the provenance and modification of documents and is among the typical artifacts considered in an e-forgery investigation. Such relevant embedded metadata often is stripped out of a native document when it is rendered into a .tiff image or .pdf file, making production of the native version critical.

B. Information Available from Computers and Electronic Media Generally

13. While some information relevant to authenticity can be extracted from individual files, much more such information is available from an inspection of all of the computers or electronic media on which the files were created, viewed, stored, or modified. Critical information relating to backdating or e-forgery can be gleaned from a computer's file system; a computer's application, security, and event logs; the metadata on unrelated files; and the

unallocated space of digital media, including a computer's hard drive, to name just a few locations.

14. Even where documents were created on another computer, an inspection of computers or digital media on which a person simply opened, viewed, or saved the documents can provide significant information about the authenticity of those documents. This is because the mere act of opening a document on a computer can create a cached version of that document on the computer's hard drive. In e-forgery matters, I have sometimes found cached versions of a document that are inconsistent with the proponent's view of the authenticity.

15. Full inspection of each computer is accomplished first by performing a digital forensic copying (or imaging) of the computer's hard drive or hard drives and other digital media used with that computer. This is an entirely passive process and does not change any of the data on the drive or media. Digital forensic examiners perform their analyses from these digital forensic images, not the originals. A typical imaging of a laptop or desktop computer, or an external hard drive, takes between one and several hours. Once the digital forensic imaging process is complete, the computers can be returned to the owners for resumed usage.

16. For the reasons set forth above, it is critical to Stroz Friedberg's analysis of the authenticity of the Purported Contract and the Purported Emails that Stroz Friedberg create: (a) forensically-sound copies of all native electronic versions of the Purported Contract and the Purported Emails; and (b) forensically-sound copies of all computers and electronic media within Mr. Ceglia's possession, custody, or control, including the computers found at his parents' house on which Mr. Ceglia claims to have found the copies of the Purported Emails on which he now relies.

A Possible Protocol for Digital Forensic Analysis

17. Typically, when the proponent of the authenticity of a document, such as Mr. Ceglia, is producing his computers and electronic media for inspection, Stroz Friedberg utilizes a protocol to protect private or privileged information. That protocol allows the digital forensic examiner to look at and rely on any information on the computers in conducting his or her authenticity examination. However, to protect private or privileged materials, the descriptions of such files or text should be redacted or masked in Stroz Friedberg's report. To accomplish this, in advance of writing the report or communicating with its client, Stroz Friedberg tenders to counsel for the owner of the computers ("Opposing Counsel") all file names, strings, fragments, and text that it intends to rely on in its report on authenticity. Opposing Counsel then can interpose an objection if any such file names, strings, fragments, or text from the computers are private or privileged. For any material objected to by Opposing Counsel, Stroz Friedberg uses a protocol to redact the content while still relying on the important metadata or other attributes.

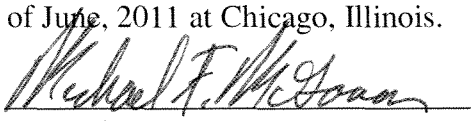
18. In addition, Stroz Friedberg's protocols incorporate a strict non-disclosure agreement to prevent it from disclosing, outside of its report, information from the computers. In sensitive cases, Stroz Friedberg even has conducted our examination at Opposing Counsel's offices, and under the supervision of Opposing Counsel's digital forensic expert, so that Stroz Friedberg does not ever have possession of the opposing party's digital forensic images and so that the opposing expert can verify that there is no inappropriate copying of data by Stroz Friedberg. Indeed, Stroz Friedberg's protocols normally require that the computers used for the inspection have no access to the Internet. As further protection, the digital forensic images can be secured in a media safe in a separately keyed room in between inspection sessions and only removed from the safe in the presence of both parties.

Conclusion

19. Stroz Friedberg should create: (a) forensically-sound copies of all native electronic versions of the Purported Contract and the Purported Emails; and (b) forensically-sound copies of all computers and electronic media within Mr. Ceglia's possession or control,

including the computers found at his parents' house on which Mr. Ceglia claims to have found the copies of the Purported Emails on which he now relies. In addition, Stroz Friedberg should be allowed to fully analyze these forensically-sound copies.

I declare under penalty of perjury that the foregoing is true and correct. Executed on this 1st day of June, 2011 at Chicago, Illinois.



Michael F. McGowan

EXHIBIT A

STROZ FRIEDBERG

MICHAEL F. MCGOWAN

DIRECTOR, DIGITAL FORENSICS

PROFESSIONAL EXPERIENCE

STROZ FRIEDBERG, LLC
Director, Digital Forensics, April 2006 to Present
Assistant Director of Computer Forensics, February 2004 to April 2006
Consultant and Computer Forensic Examiner, June 2003 to February 2004
New York, NY

Responsible for co-managing the firm's digital forensics, cyber-crime response, and electronic discovery operations. Conduct cyber-crime investigations, including investigations of network intrusions, anonymous and harassing e-mails, and thefts of trade secrets. Perform forensic examinations and acquisitions of electronic media, including computer hard drives, backup tapes, and mobile phones. Supervise and perform large-scale electronic discovery assignments for major law firms, including on-site preservation and searching in Europe, Latin America, and Asia. Respond to significant breaches of confidential and personally identifiable information. Lead efforts to investigate and remediate, to the extent possible, lapses in litigation holds. Perform statistical analyses and data analytics of disparate data sets. Provide expert witness testimony in civil and criminal cases. Significant cases include:

- Located, preserved, and forensically analyzed the metadata of a smoking-gun electronic memorandum in the Enron "Barge" investigation. Testified at trial.
- Conducted forensic investigations of several laptop computers. Authored an expert opinion proving that the subject of an internal corporate investigation backdated a key memorandum accusing a rival banker of violations of the Foreign Corrupt Practices Act.
- Participated in the design and implementation of an anti-money laundering transaction monitoring database and data analytics on behalf of an international bank in connection with a criminal investigation by the Department of Justice and Federal Reserve. Performed data analysis and helped develop an automated transaction monitoring system.
- Preserved and analyzed web, event, and domain logs to determine whether a SQL injection attack compromised customer credit card and identity information.
- Conducted source code review and digital forensic examination pursuant to an adverse-party inspection order in a litigation concerning the alleged theft of high-frequency algorithmic trading code.
- Led efforts to reconstruct and forensically analyze more than two terabytes of data in response to one of the largest potential exposures of personally identifiable information.

32 Avenue of the Americas, 4th Floor, New York, NY 1001

Tel: 212.981.6532 ■ Fax: 212.981.6545 ■ mmcgowan@strozfriedberg.com ■ www.strozfriedberg.com

STROZ FRIEDBERG

MICHAEL F. MCGOWAN

DIRECTOR, DIGITAL FORENSICS

- Pioneered a methodology for searching Korean-language documents, e-mails, and e-mail attachments for a response to a criminal grand jury subpoena in a price-fixing investigation. Conducted on-site processing to facilitate attorney review and to protect the confidentiality of sensitive client documents.

- Performed restoration of data from legacy backup tapes and data analysis in conjuction with a Medicare fraud investigation. Conducted analysis to identify instances in which medical procedures were improperly submitted as separate claims to increase the amount of reimbursement from Medicare.

- Forensically analyzed multiple computers to determine whether proprietary information and customer lists were transferred without authorization. Determined, based on a metadata analysis of the employee's recovered USB drive, that the employee had downloaded hundreds of proprietary documents in the weeks leading up to his resignation and subsequently used that information at his new place of employment. Submitted an affidavit in support of a temporary restraining order, which was corroborated by the defendant's confession under oath.

- Investigated a lapse in a major media company's e-mail retention system. Provided an assessment of the quantity of e-mail traffic that was not captured based on an analysis of e-mail server logs.

- Analyzed e-mail communications between parties in a theft of trade secrets litigation and determined that many of the alleged confidential documents were openly exchanged in e-mail correspondence prior to the litigation. Testified in Connecticut Superior Court regarding that analysis.

EDUCATION

UNIVERSITY OF CHICAGO
B.A. Economics and Statistics with General Honors, 2003

TRAINING

STROZ FRIEDBERG, LLC, 2003 to Present
In-House Training
Attend and present at regular in-house training presentations on digital forensics, cyber-crime response, computer security, and network digital forensic tools, and relevant legal topics.

HTCIA INTERNATIONAL CONFERENCE, 2010
Attended lectures concerning mobile device forensics and incident response.

32 Avenue of the Americas, 4th Floor, New York, NY 1001

Tel: 212.981.6532 ■ Fax: 212.981.6545 ■ mmcgowan@strozfriedberg.com ■ www.strozfriedberg.com

STROZ FRIEDBERG

MICHAEL F. MCGOWAN

DIRECTOR, DIGITAL FORENSICS

DIGITAL FORENSIC RESEARCH WORKSHOP, 2007
Attended annual conference on current digital forensic research.

SANS INSTITUTE, 2007
Hacker Techniques, Exploits & Incident Handling
Attended training course on identifying computer vulnerabilities and responding to computer incidents.

SANS INSTITUTE, 2005
System Forensics, Investigation & Response
Attended training concerning digital forensics and incident response covering file system structures, network response, and malicious code review.

GUIDANCE SOFTWARE, INC., 2003
EnCase Intermediate Analysis and Reporting
Attended core training course on general digital forensics issues and the use of Guidance Software's EnCase digital forensic software to analyze electronic data.

CERTIFICATIONS

EnCase Certified Forensic Examiner (EnCE)

PUBLICATIONS

November 2007: Co-authored "Electronic Discovery Behind Enemy Lines: Inspection Of An Adversary's Network Pursuant To FRCP 34(a)" in Metropolitan Corporate Counsel.

October 2006: Co-authored "Lost Back-up Tapes, Stolen Laptops and Other Tales of Data Breach Woe" in Computer and Internet Lawyer.

September 2005: Co-authored "Electronic Discovery Technology" in Adam Cohen and David Lender's treatise Electronic Discovery: Law and Practice.

May 2004: Co-authored "Your Company's Computer System" in E-Discovery: A Guide for Corporate Counsel by Sills Cummins Epstein & Gross P.C.

LECTURES

September 2010: Delivered a lecture titled "Social Networking Forensics" at the High Techology Crime Investigation Association's International Conference in Atlanta, GA.

32 Avenue of the Americas, 4th Floor, New York, NY 1001

Tel: 212.981.6532 ■ Fax: 212.981.6545 ■ mmcgowan@strozfriedberg.com ■ www.strozfriedberg.com

STROZ FRIEDBERG

MICHAEL F. MCGOWAN

DIRECTOR, DIGITAL FORENSICS

June 2010: Participated in a panel discussion on evidentiary issues regarding social networking websites hosted by the New York City chapter of Women in E-Discovery.

May 2010: Delivered a lecture at the Cyber Security and Applications seminar at Fordham University.

April 2010: Delivered a lecture titled “Web Browsing: Neither Discreet Nor Discrete” at the Computer Forensic Show.

April 2009: Co-presented a lecture titled "Digital Forensics in Business Use: A Case Study in Recovering DNA from a Hard Drive” at the John Jay Center for Cybercrime Studies.

April 2008: Delivered a lecture titled “E-Discovery and IP Theft” to the New York chapter of InfraGard.

May 2007: Co-presented at a a seminar for the Business Law Section of the New York State Bar Association titled "Hidden Data: Its Dangers and Traps for the Unwary.”

TESTIMONY

May 2010: Provided deposition testimony as a digital forensics expert in Donald G. Drapkin v. MAFCO Consolidated Group, Inc., 09 Civ. 1285 (PGG) and MacAndrews & Forbes LLC v. Donald G. Drapkin, 09 Civ. 4513.

December 2009: Testified as a digital forensics expert in Suryawanshi et al. v. UBS AG et al., FINRA Arbitration (FINRA No. 09-02568).

April 2009: Provided deposition and court testimony as a digital forensics expert in Flying Disc Investments L.P., et al., v. Baker Communications Fund II, L.P., et al., Super. Ct. of Cal. (CGC 05447294).

June 2007: Testified as a digital forensics expert in U.S. v. Zafar, 06-CR-289 (E.D.N.Y.).

July 2005: Testified as a digital forensics expert in Wall Street Network LTD v. The New York Times Co., et al., Super. Ct. of Cal. (BC 304596).

December 2004: Testified as a digital forensics expert in Gerner, et al. v. Applied Indus. Materials Corp., et al., Super. Ct. Conn.

October 2004: Testified as a digital forensics expert in U.S. v. Bayly, et al., H-03-cr-363 (S.D. Tex.).

32 Avenue of the Americas, 4th Floor, New York, NY 1001

Tel: 212.981.6532 ■ Fax: 212.981.6545 ■ mmcgowan@strozfriedberg.com ■ www.strozfriedberg.com

STROZ FRIEDBERG

MICHAEL F. MCGOWAN

DIRECTOR, DIGITAL FORENSICS

June 2004: Testified regarding a digital forensics protocol in Adkins v. General Motors Corp., et al., 03 CV 3613 (JS) (E.D.N.Y.).

June 2004: Testified as a digital forensics expert in Philip Morris USA, Inc. v. Otamedia, Ltd., 02 Civ. 7575 (GEL) (S.D.N.Y.).

PROFESSIONAL AFFILIATIONS

Member, American Statistical Association

Member, American Society for Information Science and Technology

Member, Association for Computing Machinery

11/10

32 Avenue of the Americas, 4th Floor, New York, NY 1001

Tel: 212.981.6532 ■ Fax: 212.981.6545 ■ mmcgowan@strozfriedberg.com ■ www.strozfriedberg.com

EXHIBIT B

STROZ FRIEDBERG

ERIC M. FRIEDBERG

CO-PRESIDENT

PROFESSIONAL EXPERIENCE

STROZ FRIEDBERG
Co-President
New York, NY
Joined firm January 2001

Responsible for overall management of international consulting and technical services firm with offices in New York, Washington D.C., Los Angeles, London, Boston, Dallas, San Francisco, and Minneapolis, specializing in digital forensics, cyber-crime and data breach response, electronic discovery, and business intelligence and investigations. Led M&A processes for identifying, acquiring, and integrating Docuity, Inc. (an electronic discovery processing and hosting company) and Data Genetics International, L.P. (a U.K. digital forensics firm). Negotiated and structured major private equity investments made in Stroz Friedberg by Green Capital Partners ($30mm, 2007; $7mm follow-on, 2008) and New Mountain Capital ($115mm, 2010).

National leader in responding to all forms of computer crime and abuse, including cyber-extortions, theft of trade secrets, industrial and state-sponsored espionage, leaks of confidential information, hacks and unauthorized access, denial of service attacks, illegal electronic surveillance, domain name hacks, key-logging, and Internet-based harassment.

Has managed numerous digital forensic assignments for major law firms, corporations, and government agencies in criminal, civil, regulatory, and internal corporate matters, including cases involving alleged wiping and mass deletion of data; spoliation, e-forgery, and backdating; computer-enabled theft of trade secrets; and espionage, illicit images, harassment, and hacking.

Leader in electronic discovery consulting; author of book chapters and scholarly articles on eDiscovery strategy and technology. Has managed numerous electronic discovery projects in civil and regulatory proceedings, many of which were global in scope and required the preservation, processing, and production of electronic data from hundreds of computers, servers, cell phones and PDAs, backup tapes, enterprise databases, and removable media.

Court-appointed consultant to the Special Master in *Advanced Micro Devices v Intel Corp*., No. 05-441-JJF (D. Del.); court-appointed third-party electronic discovery/digital forensics expert in *Four Seasons Hotels v Consorcio Barr,* No. 01-4572-CIV (S.D. Fla.); and *Harvest Court v Nanopierce*, No. 602281-01 (New York Supreme Court).

Significant matters include:

- Led digital forensics team that analyzed the proprietary source code behind Google's WiFi router-mapping software. Lead writer of report to world-wide Data Privacy Authorities, the F.T.C., and the public

32 Avenue of the Americas, 4th Floor, New York, NY 10013

Tel: 212.981.6536 ■ Fax: 212.981.6545 ■ efriedberg@strozfriedberg.com ■ www.strozfriedberg.com

addressing concerns that the source code captured private user communications and data. See:

http://static.googleusercontent.com/external_content/untrusted_dlcp/www.google.com/en//googleblogs/pdfs/friedberg_sourcecode_analysis_060910.pdf

- Led four-year effort to preserve, cull, search, and produce ESI for an insurance company in response to an Attorney General's criminal subpoenas and related civil actions. Oversaw preservation and production of data from hundreds of custodians, servers, and other data sources. Served as company's 30(b)(6) witness in securities class action law suit. Provided strategic advice, affidavits, and testimony regarding reasonableness of preservation and production efforts.

- Solved case in which ex-employees were for six months remotely accessing without authorization the e-mail of the Chairman, legal counsel, and in-house investigator of a public company. Oversaw development and production of evidence, including log analysis; initiated and conducted liaison with U.S. Secret Service, which led to prosecution and conviction of the offender.

- Led digital forensics team in analysis of an investment banker's multiple laptop computers, determining that a critical memorandum accusing another banker of foreign corrupt practices violations was forged. Expert report led investment banker to confess.

- Led digital forensic team in analyzing an intrusion into an FTP server on which protected customer identity data was stored. Concluded that intruder did not access customer data, facilitating decision by company to not report under data breach notification statutes.

- Led investigative team in determining who leaked sensitive internal company e-mails and information to Wall Street analysts covering the company. Oversaw forensic analysis of subjects' computers and matched snail-mailed information received by analysts to data on the computer of a single subject within the corporation. Oversaw linguistic analysis of snail-mailed cover letter to analysts. Matched linguistic anomalies to anomalies in known writings of the subject. Oversaw private investigation which led to a postal clerk who identified the subject's father as the person who snail-mailed the letters in question.

- Led digital forensic examination of two laptop computers belonging to a CFO in an internal investigation into "trading with the enemy" allegations. Established that just before he relinquished his computers to investigators, the CFO deleted folders relating to trading with Iran. Conclusions supported termination for cause.

ERIC M. FRIEDBERG

CO-PRESIDENT

- Oversaw preservation, culling, and processing of laptop, desktop, server, PDA, and removable media data from over 60 lawyers and paralegals in six of a major law firm's domestic offices, in response to a threatened malpractice case. Developed a methodology for conducting an electronic discovery project within a law firm environment, where there are unique issues relating to commingled, privileged data.

- Oversaw development of proprietary techniques to conduct key-word search of Korean-language data in an antitrust inquiry. Oversaw the establishment of an on-site laboratory in Seoul to facilitate confidential data processing.

- Oversaw multi-year electronic discovery project for Audit Committee of a public company in an accounting fraud scandal. Gathered and processed data from over 550 custodians for response to regulatory and civil subpoenas. Conducted deep forensic analysis relating to possible illegal destruction of data.

- Led cyber-crime response team in identifying location within a corporate network of illegally installed "sniffer" program that was covertly capturing corporate instant message traffic. Led forensic team in analyzing laptop on which sniffer was running to identify internal employees who installed sniffer and accessed sniffed IMs. Conducted interviews of multiple IT staff members, obtaining confessions from some and exonerating others in illegal scheme.

UNITED STATES ATTORNEY'S OFFICE, E.D.N.Y.
Senior Litigation Counsel, November 1999 to December 2000
Computer and Telecommunications Coordinator, December 1997 to December 2000
Chief, Narcotics Unit, December 1994 to November 1997
Deputy Chief, Narcotics Unit, January 1993 to November 1994
Line Assistant, April 1989 to December 1992
New York, NY

As Computer and Telecommunications Coordinator:

- Investigated and prosecuted cases involving computer hacks, denial of service attacks, Internet-related trade secret theft, criminal trademark and copyright infringement, computer hardware and software counterfeiting, telecommunications billing fraud, and illegal electronic surveillance.

- Participated in the establishment of enforcement policy, built relationships with client agencies, and supervised up to five Assistant U.S. Attorneys.

32 Avenue of the Americas, 4th Floor, New York, NY 10013

Tel: 212.981.6536 ■ Fax: 212.981.6545 ■ efriedberg@strozfriedberg.com ■ www.strozfriedberg.com

- Investigated telecommunications fraud case using one of the first government e-mail wiretaps.

As Chief of Narcotics and in other positions:

- Investigated, litigated, and handled appeals of complex cases involving narcotics trafficking, money laundering, drug-related violence, racketeering, securities fraud, and public corruption. Numerous trials, ranging from one to eight weeks in length.

- Participated in the establishment of narcotics and money laundering enforcement policy, built relationships with client agencies, and supervised up to 15 Assistant U.S. Attorneys and two Deputy Chiefs.

- Received 1994 Department of Justice Award for Superior Performance for investigation and prosecution of six accomplices in Cali Cartel-ordered assassination of Manuel de Dios Unanue, the former editor-in-chief of *El Diario*.

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
Associate Attorney, Litigation Department
New York, NY
1983 to 1989

Participated in all phases of intellectual property, takeover, general commercial, and product liability litigation, including two jury trials and several preliminary injunction hearings.

EDUCATION

BROOKLYN LAW SCHOOL
J.D. 1983, *magna cum laude*

BRANDEIS UNIVERSITY
B.A. Philosophy, 1978, *cum laude*
Varsity soccer, 1973, 1974, 1975

PUBLICATIONS

March 2008: *New Electronic Discovery Teams, Roles & Functions*, a white paper published by The Sedona Conference.

October 2006: Co-authored “Lost Back-up Tapes, Stolen Laptops and Other Tales of Data Breach Woe,” an article published in *Computer and Internet Lawyer.*

September 2005: Co-authored “Electronic Discovery Technology,” Chapter Nine in Adam Cohen and David Lender's treatise *Electronic Discovery: Law and Practice.*

July 2005: *To Recycle or Not to Recycle, That Is The Hot Backup Tape Question,* a white paper published in the Practicing Law Institute's Fifth Annual Municipal Law Institute course materials.

May 2004: Co-authored “Your Company’s Computer System,” Chapter One in the book *E-Discovery: A Guide for Corporate Counsel*, published by Sills Cummis Epstein & Gross P.C.

January 2004: “To Cache a Thief: How Litigants and Lawyers Tamper with Electronic Evidence and Why They Get Caught,” an article published in *The American Lawyer* magazine.

November 2003: Co-authored “21st Century Forensics: Searching for the 'Smoking Gun' in Computer Hard Drives,” an article published in *The Prosecutor*, the monthly publication of the National District Attorneys Association.

LECTURES

July 2010: Led Information Systems Security Association (ISSA) industry webinar entitled “Social Networking Forensics”.

January 2009: Presented a lecture entitled “New Electronic Discovery Teams, Roles, & Functions” at the Association of the Bar of the City of New York.

2008: Participated in a panel discussion entitled “Digital Forensics: From Investigation to the Courtroom” at the Cyberlaw: Expanding the Horizons Conference, hosted by the American Bar Association in Washington, DC.

June 2008: Participated in a panel discussion entitled “Data Breach Investigation and Response” at the Practical Privacy Series, hosted by the International Association of Privacy Professionals (IAPP).

May 2008: Led a panel discussion entitled “Barbarians at the Cybergate” at the New York CIO Executive Summit.

May 2008: Participated in a panel discussion entitled “Forensics, an Executive Overview” at the CISO Executive Forum, hosted by the Information Systems Security Association (ISSA).

April 2008: Participated in a panel discussion entitled “E-Discovery in Insurance” at the Electronic Discovery Seminar, hosted by DRI.

STROZ FRIEDBERG

ERIC M. FRIEDBERG

CO-PRESIDENT

March 2008: Participated as a Faculty Member for the Sedona Conference Institute event in San Diego, California, entitled "Second Annual Program on Getting Ahead of the e-Discovery Curve: Strategies to Reduce Costs and Meet Judicial Expectations" and as a panel member for presentations entitled "New Roles and New Teams to Meet ESI Production Obligations/ Expectations" and “Effective Preparation by Requesting Party for Rule 26 (f) Conferences.”

January 2008: Led a panel discussion entitled “Electronic Discovery: Technology, Strategy & Emerging Standards” at the Association of the Bar of the City of New York.

November 2007: Participated in a panel discussion entitled “Preservation: From Legal Holds to Preservation Methodologies” at the Advance E-Discovery Technology Workshop at Georgetown University Law Center.

September 2007: Led a panel discussion entitled “Cyber-crime: The Insider Threat” for the New York Chapter of the Association of Corporate Counsel of America (ACCA).

June 5, 2007: Delivered a lecture on “The Challenges Confronting the Digital Forensics Community” to The National Academies' Committee on Identifying the Needs of the Forensic Sciences Community.

June 2007: Participated in a panel discussion for The Association of Corporate Counsel of America (ACCA) 2007 Ethics Marathon at Pfizer Corp.

June 2007: Participated in a panel discussion entitled “Computer Forensics and Auditing” for the ABA.

March 29, 2007: Participated as a Faculty Member for the Sedona Conference Institute event in Memphis, Tennessee, entitled "Getting Ahead of the e-Discovery Curve: Strategies for Companies & Their Counsel to Reduce Costs and Meet Judicial Expectations" and as a panel member for a presentation entitled "Changing Corporate Culture: Creating & Managing New Relationships to Effectively Respond to Discovery & Investigations."

February 21, 2007: Led a panel discussion entitled "Compliance: Using Computer Forensics to Ensure Process/Protocol" for the members of the Greater New York Chapter of the ACCA.

December 6, 2006: Participated in a panel discussion entitled “Fundamentals of e-Discovery” for the New York State Bar Association.

December 5, 2006: Participated in a panel discussion entitled “Identity Theft: Understanding the New Laws and Ways to Protect Your Clients and Yourself from Becoming a Victim” at the Association of the Bar of the City of New York.

32 Avenue of the Americas, 4th Floor, New York, NY 10013

Tel: 212.981.6536 ■ Fax: 212.981.6545 ■ efriedberg@strozfriedberg.com ■ www.strozfriedberg.com

STROZ FRIEDBERG

ERIC M. FRIEDBERG

CO-PRESIDENT

November 29, 2006: Participated in a webinar entitled “Proskauer on Privacy: The Government and Privacy.”

November 10, 2006: Participated in a panel discussion entitled “Forensics in e-Discovery” at Georgetown University Law Center.

November 6, 2006: Delivered a lecture entitled “Data Breach Notification: Technology, Strategy, and Law” to the members of the ACCA of Greater N.Y.

March 16, 2006: Delivered a lecture entitled "Computer Forensics: Technology, Strategy and Law" to the Communications and Media Law Committee of the New York City Bar Association.

February 2, 2006: Delivered a lecture entitled "Computer Forensics: Technology, Strategy and Law" at Brooklyn Law School.

March 16, 2005: Delivered a lecture entitled "Computer Forensics: Technology, Strategy and Law" to the Communications and Media Law Committee of the New York City Bar Association.

October 27, 2005: Participated in a panel discussion on "Electronic Discovery in Litigation and What It Means for the European Company" at the Fall 2005 meeting for the International Section of the American Bar Association.

July 27, 2005: Gave a presentation on "Electronic Discovery" for the Practicing Law Institute's Fifth Annual Municipal Law Institute.

April 6, 2005: Participated in a panel presentation with Hon. Shira A. Scheindlin, U.S. District Judge, Southern District of New York; Hon. Ira Warshawsky, Supreme Court Judge, Nassau County; and David J. Lender, Esq., Weil Gotshal & Manges LLP, on "E-Discovery: The Basics and Beyond" at the New York State Judicial Institute.

February 23, 2005: Delivered a lecture entitled "Computer Forensics in Support of Litigation" to the Association of the Bar of the City of New York

January 12, 2005: Gave a presentation entitled "Handling Child Pornography Discovered During a Forensic Examination" at the Quarterly Meeting for the New York Electronic Crimes Task Force (NYECTF) of the U.S. Secret Service and John Jay College of Criminal Justice.

October 1, 2004: Delivered a lecture entitled “To Cache a Thief: E-Evidence Tampering," which addressed using computer forensics to determine whether electronic documents were tampered with or are authentic, at the Association of Legal Administrators Region 5 Educational Conference.

STROZ FRIEDBERG

ERIC M. FRIEDBERG

CO-PRESIDENT

EXPERT TESTIMONY

November 2007: Testified as a 30(b)(6) witness for American International Group in a securities class action.

PRO BONO

Member, Advisory Committee to the President of Brooklyn Law School. Advise President on strategic issues relating to positioning, marketing, recruiting, retention, and fundraising.

Consultant to the Global Network Initiative (GNI), an international consortium of communication and information providers, human rights groups, and academics committed to upholding global human rights norms, privacy rights, and freedom of expression in the electronic sharing and transmission of information. Assist GNI in developing a practical mechanism to monitor members' compliance with GNI principles without compromising private information, legitimate government requests for information, and efficient business functions. Advise on impact of domestic and foreign privacy laws, including ECPA, FISA, Title III, grand jury secrecy laws, and law enforcement power to compel secrecy, including in connection with search warrants, grand jury subpoenas, criminal and national security wiretaps, and NSLs.

PROFESSIONAL AFFILIATIONS

- Member, International Association of Privacy Professionals
- Former member, The Sedona Conference Working Group on Electronic Discovery
- Former member, E-Discovery Subcommittee of the New York State Bar Association's Commercial and Federal Litigation Section
- Former Member, Information Technology Law Committee of the New York City Bar Association

32 Avenue of the Americas, 4th Floor, New York, NY 10013

Tel: 212.981.6536 ■ Fax: 212.981.6545 ■ efriedberg@strozfriedberg.com ■ www.strozfriedberg.com