

EXHIBIT B

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

CO-PRESIDENT

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.

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.

CO-PRESIDENT

- 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*.

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

CO-PRESIDENT

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 Practising 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.

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.

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.

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