THOMAS BROWN
BERKELEY RESEARCH GROUP, LLC
810 Seventh Avenue Suite 4100 | New York, NY 10019

Direct: 646.862.0979
tbrown@thinkbrg.com

SUMMARY

Thomas Brown is a Managing Director and Global Leader of Berkeley Research Group's Cyber Security and Investigations practice. He also co-leads BRG's Cryptocurrency and Digital Assets practice. Mr. Brown specializes in helping clients manage cyber risk, investigate cyber incidents and crypto-related matters, remediate vulnerabilities, and comply with cyber security, data privacy, and cryptocurrency standards and regulations. As a veteran federal prosecutor and trial lawyer with deep experience in cyber and crypto matters, Mr. Brown synthesizes and presents investigative results clearly to critical audiences, including boards of directors and regulators.

From 2002 to 2014, Mr. Brown served as an Assistant United States Attorney in the U.S. Attorney's Office for the Southern District of New York, where he supervised the Complex Frauds and Cyber Crime Unit.

As a federal prosecutor, Mr. Brown supervised and led a range of complex, cross-border cyber and cryptocurrency investigations and prosecutions, including cases against the owner of Silk Road, a $1.2 billion underground drug website, which resulted in the seizure of 173,000 bitcoin; a United States exchanger for WebMoney, the Russian-based digital currency; and the operators of Liberty Reserve, a Latin American-based convertible virtual currency.

Mr. Brown also led investigations and prosecutions of a variety of white-collar offenses, including economic espionage and theft of trade secrets, money laundering, FCPA violations, securities fraud, bankruptcy fraud, identity theft, criminal copyright theft, and tax fraud, among other violations. In addition, Mr. Brown developed an innovative strategy to combat online copyright piracy, pioneering an international intellectual property rights enforcement program still employed by the U.S. Departments of Justice and Homeland Security.

Besides conducting multiple jury trials and arguing a number of appeals before the U.S. Court of Appeals for the Second Circuit, Mr. Brown also won favorable judicial opinions with national impact on cyber-related issues, including an electronic surveillance matter and a case of first impression concerning the compelled production of data stored overseas by Internet service providers that led to passage of the CLOUD Act.

Mr. Brown is a recipient of the FBI Director's Award for Outstanding Cyber Investigation and was named "Prosecutor of the Year" by the Federal Law Enforcement Foundation.
Mr. Brown frequently lectures on cyber security, crypto, and data privacy issues to legal, business, and law enforcement groups.

EDUCATION

J.D., *cum laude*	University of Minnesota Law School, 1996
B.A., History, *cum laude*	Carleton College, 1991

PRACTICE AREAS

Blockchain/Digital Assets
Cyber Security Assessments and Preparedness
Cyber Incident Response and Investigations
Data Privacy Compliance and Best Practices
Digital Forensics
White Collar Investigations

PROFESSIONAL AFFILIATIONS

Federal Bar Council
New York City Bar Association

REPRESENTATIVE MATTERS – PRIVATE PRACTICE

Cryptocurrency/Blockchain

- **DeFi Platform.** Assisted a decentralized credit-based stablecoin issuer with a law enforcement referral following an attack that resulted in the theft of more than $80 million in user assets.
- **Non-Fungible Token Marketplace.** Conducted a cyber security and forensic accounting investigation of a credential stuffing attack that resulted in the theft of NFTs and cryptocurrency tokens from a major NFT exchange. Investigative results, including an analysis of the total monetary loss, movement of crypto assets between wallets, and the client's response to the attack, were used to support a successful presentation to the FTC by counsel.
- **U.S. Department of Justice.** Provided technical cyber investigative assistance to a federal criminal prosecution of a global cryptocurrency Ponzi scheme that stole money from thousands of victims. The engagement included an analysis of cryptocurrency wallets and transactions, as well as the forensic investigation of a website and databases used by the defendants to facilitate the criminal scheme.
- **Stablecoin Issuer.** Performed an independent, multi-year review of billions of dollars' worth of fiat currency backing for stable tokens for counsel for a major stablecoin issuer in connection with multiple regulatory investigations. The review also involved a parallel accounting of token issuance over time. Investigative report was used by counsel to respond to regulators' inquiries.
- **U.S. Department of Justice.** Analyzed a large volume of bitcoin transactions for the U.S. Attorney's Office for the Southern District of New York in connection with a claim arising from a cryptocurrency forfeiture action.

- **U.S. Department of Justice.** Analyzed bitcoin transactions underlying more than $1 billion worth of illegal narcotics deals on the Silk Road online black market in connection with the trial of Silk Road's owner and operator, Ross Ulbricht.
- **U.S. Department of Justice**. Assisted with the investigation of a multi-billion dollar European and Middle Eastern-based pyramid scheme involving the sale of fraudulent cryptocurrency using a private blockchain, as well as provided investigative support for the trial of one of the scheme's participants.

Cyber Security

- **Defendant in High-Profile Federal Prosecution/Trial**. Provided expert cyber security-related litigation consulting to counsel representing the defendant in a high-profile federal criminal investigation and trial.
- **Telecommunications Company.** Assist counsel with a referral to and ongoing coordination with federal law enforcement regarding a ransomware attack that stole millions of dollars from the client company.
- **U.S. Government Agency.** Ongoing independent investigation of the scope and impact of a database access control issue. The engagement involves multi-year forensic review of access logs, witness interviews, and review of associated documents.
- **Retail Electricity Provider.** Spearheaded the rapid response to a Conti ransomware attack that shut down the client's networks shortly before the closing of another company's acquisition of the client. Organized parallel investigative, legal and ransom payment responses; advised the client company's CEO on best practices in connection with ransomware attacks; and assisted legal counsel with cyber security issues relating to the pending acquisition, as well as issues relating to the ransom payment and potential litigation and privacy notifications. Coordinated a referral to and communications with federal law enforcement.
- **Global Payment Processor.** Led an independent root cause investigation of a software testing failure at global payment processor, which caused a large volume of erroneous ACH transactions. Prepared a report which the client provided to multiple outside banking regulators.
- **Insurance Company.** Rapid incident response and forensic investigation of a Kaseya VSA ransomware attack attributed to the REvil hacking group. Assisted client company in rebuilding its computer system from a backup, including a review of the backup for malware. Presented findings to the company's board of directors and assisted counsel in responding to questions from the New York State Department of Finance.
- **Video Game Company**. Conducted an investigation of hacking groups that targeted a high-profile video game developed and marketed by leading game publisher. Prepared a successful referral to federal law enforcement. Coordinated the relationship with law enforcement, including the client's responses to grand jury subpoenas.
- **New York Investment Advisor.** Conducted a cyber forensic investigation of unauthorized access to the client company's network, including an assessment of potential theft of personally identifiable information. Drafted a report of findings and suggestions for remediation.

- **New York Law Firm.** Conducted law firm-centric cyber and data security awareness training for hundreds of legal and non-legal staff, as well as a cyber incident table-top exercise for the client firm's leadership.
- **New York Investment Management Firm.**
    - Cybersquatting investigation involving multiple infringing domain names and websites that traded on the name and reputation of a multi-billion-dollar investment management firm and its well-known founder to engage in online fraudulent activity. Prepared cease-and-desist letters to hosting companies, as well as criminal complaints.
    - Investigated advance-fee fraudsters who used an infringing website to target and steal hundreds of thousands of dollars from victims. Prepared a successful federal criminal referral to law enforcement that resulted in the indictment of the fraudsters.
- **New York Financial Services Company.** In a pre-litigation context, investigated a man-in-the-middle email attack that manipulated communications between a securities sales and trading company and one of its clients, resulting in the company sending $3 million of client's funds to fraudulent overseas bank accounts. Presented findings to counsel for use in settlement negotiations with the client and assisted the company with remediation strategies.
- **International Luxury Retailer.** Conducted a rapid-response investigation of an ongoing phishing attack (both telephonic and using spoofed email accounts) aimed at a senior executive that caused $3.9 million in fraudulent wire transfers to be sent to a foreign bank account. Assisted in the recall of certain of the wires and coordinated with the FBI and foreign law enforcement to freeze additional funds. Drafted a comprehensive report and presented its findings to the client's General Counsel. Prepared a memorandum detailing suggested remediations to mitigate future phishing attacks.
- **International Health Care Company.** Conducted a HIPAA Security Rule risk assessment for a multi-billion-dollar retailer that sells products both online and through brick-and-mortar stores. Drafted a gap analysis and suggestions for remediation. Briefed General Counsel and Co-CEO on our findings.
- **U.S. Health Care Company.** Conducted a comprehensive and independent technical and policy-based cyber security and data privacy review of an $8.5 billion healthcare company on behalf of its board of directors following a data breach. Presented the investigation's findings to the company's CEO and board of directors. Drafted specific remediations in connection with, among other things, data collection, data minimization, access control, and web portal security.
- **U.S. Government Agency.** Investigated issues relating to the agency's IT networks.
- **Foreign-Based Banking Institution.** Conducted an audit of the bank's data security and privacy environment under FFIEC, GLBA and NIST standards. Drafted policies and procedures to ensure compliance.
- **Insurance Company.** Conduct periodic cyber security risk assessments of a large insurance company and draft reports of findings to comply with the New York State Department of Financial Services' Cybersecurity Regulation.
- **Private Equity Firm.** Cyber security and data privacy review of the firm's network, data collection and data storage practices following a data breach to comply with guidelines set by the SEC.

Drafted a report recommending prioritized remediations.

- **Capital Investment Finance Company.** Investigated a cyber security attack which resulted in the theft of $3.3 million. Traced the source of attack and prepared a report and presentation for the company's board of directors. Facilitated a law enforcement referral. Drafted remediation strategies.
- **New York Financial Services Company.** Rapid response to a data breach at a New York-based financial services company that resulted in the leak of sensitive client information in the press. Traced the source of breach, developed a remediation program, and drafted a report which was shared with regulators. Assisted legal counsel in presenting findings to an executive committee and the board of directors.
- **Global Banking Institution.** Complex root cause analysis of a critical software upgrade failure that halted daily calculations of certain asset values by the bank. Assisted legal counsel in presenting the root cause analysis to a senior executive committee, the CEO, and the board of directors. Provided expert technical consulting services for related civil litigation and regulatory inquiries.
- **Foreign-Based Educational Institution.** Conducted an investigation of a data breach that resulted in the leak of hundreds of highly confidential documents to a local newspaper, which published several articles based on leaked information. The investigation involved vulnerability testing and analysis of multiple wired and wireless networks at an overseas location, as well as complex forensic collection, restoration, processing, and review of multi-terabyte databases.
- **New York-Based Investment Management Firm.** Executive cyber security consulting.
- **International Manufacturer.** Executive cyber security consulting.
- **Family Office.** Investigation of a cyber-attack against a family investment management office, which resulted in a loss of over $1 million. Instituted a remediation program, including a security overhaul of the office's computer network.

Digital Forensics and E-Discovery

- **U.S. Department of Justice.** Provide ongoing computer and mobile device forensics and related analytical services in support of a variety of sensitive and confidential criminal grand jury investigations and civil enforcement matters. Supply ancillary investigative assistance and trial testimony, as necessary.
- **Pharmaceutical Company CEO.** Rapid on-site collection of the CEO's mobile device and iCloud account data for defense counsel following a federal securities fraud investigation.
- **Financial Services Company.** Forensic collection of data from 20+ custodians' mobile devices, as well as related e-discovery analytic services for counsel representing an electronic trading platform company in connection with a CFTC insider-trading investigation.
- **Board Chair and Controlling Shareholder.** In connection with an ongoing shareholder litigation, provide data collection and electronic discovery services to the Chair and controlling shareholder of a Fortune 500 company. Devised safe, secure, and encrypted collection methods given the sensitivity of the data sources, which included a proprietary database.
- **Individual Investment Bank Employee.** Forensic investigation of mobile devices and related databases to recover deleted instant messages in support of the employee's defense to CFTC's allegations of evidence spoliation in an insider trading case. Assisted counsel in presentations of investigative findings to the CFTC.

- **Multiple Investment Bank Employees.** Forensic investigation of mobile devices used by multiple investment bank employees. Assisted counsel in producing recovered information to the CFTC in the context of an insider trading investigation.
- **PPE Manufacturer.** Imaging and processing of mobile phones, laptops, and online accounts of employees of a PPE manufacturer in connection with DOJ fraud investigation. Assisted counsel in responding to criminal subpoenas.

White Collar

- **U.S. Department of Justice.** Provide ongoing forensic accounting and related analytical services in support of a variety of sensitive and confidential criminal grand jury investigations and civil enforcement matters. Supply ancillary investigative assistance and trial testimony, as necessary.
- **Global Bank.**
    - Led a team of accountants and analysts conducting a complex flow of funds analysis of bank and brokerage accounts in connection with the bank's defense of an action brought by a high-net worth individual and his family who allege their financial manager fraudulently transferred more than $50 million from the bank.
    - Led a large team of accountants and analysts in the independent examination of up to 10 years' worth of account records for 15,000 retail customers in connection with an internal investigation of the theft and money laundering of over $3 million by bank employees. Developed data acquisition, sampling, and testing strategies. Summarized analytical results in support of the bank's response to regulators and a potential criminal investigation.
    - Led a large team of accountants and analysts in the independent review of private bank customer records in support of an internal investigation of theft of funds by a bank employee. Summarized investigative results in aid of the bank's response to regulators and a referral to law enforcement.
- **New York-Based Educational Institution.** Independent investigation of whether an electrical contracting company had completed the full scope of work on projects at five residential properties in New York City owned by the Educational Institution. In addition, evaluated potential safety hazards, including potential violations of applicable safety codes and standards. Prepared reports that were used in connection with a presentation to the Educational Institution's board of trustees.
- **U.S. Government Contractor.** Developed a cost-effective solution to create an electronic database of approximately 265,000 paper medical record forms from multiple overseas sources for a government contractor in connection with a U.S. Government investigation of billing fraud. Developed a coding strategy to extract over 50 fields of information per form. Detected duplicates and missing records among data sets and assisted the client in identifying additional sources of records. Supported a statistical analysis of the database.

Economic Espionage/Theft of Trade Secrets

- **Commercial Website.** Forensic investigation of a website from which commercial listings are

alleged to have been scraped by a competitor and posted on the competitor's website. Engagement involved the analysis of client website code and the investigation of scraping techniques employed by the competitor.

- **Oil and Gas Sector Company.** Economic espionage investigation at a multi-billion-dollar oil and gas services company. Instituted an efficient and cost-effective monitoring program, which resulted in the detection of theft of trade secrets by company employees, two referrals to the FBI (one national security-related and the other criminal), and the recovery of valuable proprietary technology. In addition, conducted a cyber security review of the company's networks and policies, presented the results of those findings to the CEO and Board of Directors, and created an information security improvement plan.

REPRESENTATIVE MATTERS – GOVERNMENT SERVICE

Mr. Brown investigated and prosecuted a broad range of criminal conduct, including many cutting-edge cases, during his tenure as a federal prosecutor. Several of those prosecutions were named among the FBI's annual list of "Top 10" cases. The following are representative matters handled by Mr. Brown during his government service:

Cryptocurrency/The Dark Web

- **Silk Road Hidden Website.** Initiated, planned, and supervised the investigation and prosecution of Ross William Ulbricht, a/k/a "Dread Pirate Roberts," the owner and operator of Silk Road, an online black market on the Dark Web that facilitated over $1.2 billion in illegal drug sales. Silk Road hid from law enforcement by using technology that made it practically impossible to locate the computer servers hosting the site and by using Bitcoin, a digital currency as anonymous as cash. The investigation recovered approximately 173,000 bitcoins worth approximately $100 million at the time of seizure, the largest Bitcoin seizure in history. Named one of the FBI's Top 10 cases of 2013. *United States v. Ross Ulbricht*.
- **WebMoney Exchanger**. Led the investigation and prosecution of a digital currency exchanger in New York, who facilitated the transfer of millions of dollars of criminal proceeds to Russia by converting it into WebMoney, a convertible virtual currency. *United States v. Ilya Boruch*.
- **Liberty Reserve Virtual Currency**. Supervised the investigation and prosecution of Liberty Reserve, a company that operated one of the most widely used digital currency services, and seven of its principals and employees for money laundering and operating an unlicensed money transmitting business. Liberty Reserve had more than one million users worldwide, who conducted 55 million transactions and laundered more than $6 billion in suspected criminal proceeds. *United States v. Liberty Reserve, et al.*

Computer Hacking

- **Iranian Nation-State Hackers**. Initiated and supervised the investigation of members of two Iranian private security companies, ITSec Team and Mersad Co., which launched attacks on U.S. banks' websites and hacked the computer controller for a water-control dam in New York State on behalf of the Iranian Government. *United States v. Ahmad Fathi, et al.*

- **Anonymous/LulzSec**. Led the investigation and prosecution of the core leadership of the online hacktivist groups Anonymous and LulzSec, including Hector Monsegur, a/k/a "Sabu," and Jeremey Hammond, a/k/a "Anarchaos," (the FBI's most wanted cyber fugitive at the time), for hacking computer systems used by Fox Broadcasting Company, Sony Pictures Entertainment, the Public Broadcasting Service, the Arizona Department of Public Safety, and Strategic Forecasting, Inc., among hundreds of other victim entities in the government, education, financial services, travel and entertainment, technology, media, healthcare, and consumer products sectors. Anonymous's and LulzSec's hacks resulted in the disclosure of personal identifying information of over one million victims. Named one of the FBI's Top 10 cases of 2012. *United States v. Jeremey Hammond, et al.*
- **Hack of NASDAQ**. Led the investigation and prosecution of a Russian national for hacking into the NASDAQ's computer networks and installing malware that permitted access, theft, or alteration of data. *United States v. Alexsandr Kalinin, a/k/a "Grig."*
- **Operation CitiSkim**. Led the investigation and prosecution of a Russian national and his international co-conspirators for hacking an ATM network used by multiple financial institutions, including Citibank and PNC Bank, and stealing over 800,000 accounts, resulting in at least $7.8 million in losses. The investigation involved the first-ever criminal extradition from Estonia. *United States v. Nikolay Nasenkov, a/k/a "Loader," et al.*
- **Hacking/Illegal Wiretapping**. Led the prosecution of an Irish national and hacktivist for surreptitiously recording and disclosing a conference call between international law enforcement organizations. *United States v. Donncha O'Cearrbhail, a/k/a "Palladium."*
- **Hack of Federal Reserve**. Investigated and supervised the prosecution of UK national and hacktivist for hacking computer systems of the Federal Reserve Bank of New York, stealing sensitive data, and posting it on public websites. *United States v. Lauri Love.*

Malware/Botnets

- **Gozi Virus**. Led the investigation and prosecution of Russian, Latvian and Romanian nationals for creating and distributing the "Gozi" virus, malware that stole online banking credentials of millions of computer users worldwide. Named one of the FBI's Top 10 cases of 2013. *United States v. Nikita Kuzmin, a/k/a "76," et al.*
- **Operation Cardshop**. Conceived of, designed, and supervised a complex, two-year FBI undercover operation that resulted in the largest coordinated international law enforcement action in history directed at online criminals involved in the theft, trafficking, and use of stolen financial and personal identification data. Coordinated action among 13 countries resulting in 30 arrests. Operation Cardshop is credited with identifying over 400,000 compromised credit cards and preventing more than $205 million in potential losses. Named one of the FBI's Top 10 cases of 2012.
- **Operation Ghost Click/Rove Digital**. Initiated and supervised the investigation and prosecution of six Estonian nationals and one Russian national for operating a massive and sophisticated Internet advertising fraud scheme that infected with malware more than four million computers located in over 100 countries. Named one of the FBI's Top 10 cases of 2011.
- **Blackshades Malware**. Supervised the investigation and prosecution of the creators, distributors, and users of "Blackshades," a sophisticated form of malware purchased by thousands of people in more than 100 countries and used to infect more than 500,000 victim computers. Blackshades enabled users to secretly control victims' computers, hold the computers at ransom, activate web cameras, and steal file and account information. *United States v. Alex Yücel, et al.*

- **Zeus Malware**. Prosecuted a global fraud ring that used "Zeus" malware to steal more than $3 million from victims' bank accounts. Named one of the FBI's Top 10 cases of 2010. *United States v. Artem Tsygankov, et al.*

Economic Espionage/Theft of Trade Secrets

- **Theft of Trade Secrets from Société Générale**. Led the investigation and prosecution of a former Société Générale trader for stealing proprietary code used in the high-frequency trading business. *United States v. Samarth Agrawal*.
- **Theft of Trade Secrets from Federal Reserve**. Supervised the prosecution of a Chinese national for stealing proprietary software code worth nearly $10 million from the Federal Reserve Bank of New York while a contract employee there. *United States v. Bo Zhang.*

Criminal Copyright Enforcement

- **Operation in Our Sites.** In a first-of-its-kind operation, led the investigation, seizure, and forfeiture of seven domain names of websites that distributed pirated movies, television shows, and games over the Internet in violation of federal criminal copyright law. The investigation and seizures served as a basis for the U.S. Department of Justice's and U.S. Department of Homeland Security's continuing multi-jurisdictional, online anti-piracy enforcement operation coordinated through the National Intellectual Property Rights Center, which has seized thousands of infringing domain names and millions of dollars in criminal proceeds and infringing goods.

White Collar/Fraud

- ***United States v. Christoph Schlutz-Reineke, et al.*** Led the investigation and prosecution of the leader of two Manhattan investment advisory firms and his accomplices for a securities fraud scheme that defrauded more than 500 investors of $28 million.
- ***United States v. Clyde Hall, et al.*** Led the investigation and prosecution of a former New York Giants football player for investment and bankruptcy fraud schemes that stole more than $25 million from victims.
- ***United States v. Ernest Vogliano.*** Prosecuted a United States resident who used Liechtenstein and Hong Kong shell companies to hide $4.9 million at UBS Bank in Switzerland as part of a tax fraud scheme.
- ***United States v. Eric Klein, et al.*** Prosecuted an attorney for his participation in a fraud scheme to obtain fees for purported start-up capital.
- ***United States v. Dominick Colasuonno and Philip Colasuonno.*** Prosecuted principals of a check cashing business for accounting fraud.

SIGNIFICANT JUDICIAL OPINIONS

- Obtained a favorable decision in a case of first impression involving the compelled disclosure of data stored overseas by Internet service providers. *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*,15 F. Supp. 3d 466 (SDNY 2014) (Francis, MJ), *rev'd*, 829 F.3d 197 (2d Cir. 2016), *cert. granted*, 583 U.S. ___ (2017), *vacating as moot in light of the Clarifying Lawful Overseas Use of Data Act (Cloud Act), Pub. L. 115-141*, 584 U.S. ___ (2018).
- Successfully litigated a significant electronic surveillance issue with national impact using a novel legal theory, resulting in two widely cited cases, *In re Applic. of U.S. for an Order for Disclosure*, 405 F.Supp.2d 435 (SDNY 2005) (Gorenstein, MJ) and *In re Applic. of U.S. for an Order for Prospective Cell Site Location Information*, 460 F.Supp.2d 448 (SDNY 2006) (Kaplan, J).

HONORS AND AWARDS

- FBI Director's Award for Outstanding Cyber Investigation for the successful investigation and prosecution of an international criminal organization that stole millions of dollars through a sophisticated cyber-attack on United States banking infrastructure.
- Federal Prosecutor of the Year Award, Federal Law Enforcement Foundation for developing and expanding the cyber and intellectual property crime enforcement program at the United States Attorney's Office for the Southern District of New York and for innovative use of online investigative techniques.

SELECTED PRESENTATIONS

- Panelist, “War in Ukraine – Impacts on the Energy Industry, Cybersecurity & Sanctions Enforcement,” WSG North America Regional Council – Webinar, June 2022
- Panelist, “Understanding Cryptocurrency – from Investment to the Environmental Impact,” Carleton College Alumni Clubs – Webinar, March 2022
- Speaker, “GDPR Compliance in India,” 5th Edition LawServ – Mumbai, India, February 2020
- Faculty, “Successful Prosecutions in the Digital Age,” National Advocacy Center, United States Department of Justice – Columbia, SC, August 2019
- Convocation Speaker, “Cutting-Edge Solutions to Address Complex Cyber Threats,” Carleton College – Northfield, MN, April 2019
- Panelist, “SEC Cybersecurity Enforcement,” Practicing Law Institute – New York, NY, February 2019
- Faculty, U.S. State Department-Sponsored Cybercrime Investigations Training for Lebanese Judges and Law Enforcement Officers – Beirut, Lebanon, September 2018
- Lecturer, “Cybercrime Prosecutions in the United States: An Overview,” Duke Law School – Durham, NC, September 2018
- Panelist, “Emerging Tech Crimes: Going Dark, Bug Bounties and Synthetic ID Theft,” National Association of Attorneys General Summer Meeting – Portland, OR, June 2018.
- Panelist, “War Games: Real World Cybersecurity Data Breach Simulation,” Hispanic National Bar Association’s Corporate Counsel Conference – San Francisco, CA, March 2018
- Panelist, “Cybersecurity, Privacy, and the Many Mysteries of Data for Life Sciences Companies,” 2018 Compliance & Cybersecurity Forum, Seton Hall Law School – Newark, NJ, February 2018
- Faculty, “New York’s Cybersecurity Regulation: Sarbanes Oxley Meets Cyber?” Privacy + Security Forum, George Washington University – Washington, D.C., October 2017
- Lecturer, “Disentangling Yourself from the Dark Web and Virtual Currencies: Challenges Prosecutors and Investigators Face in the Modern Era,” National Attorneys General Training & Research Institute, International Fellows Program – Washington, D.C., June 2017
- Keynote Speaker, “The Evolving Cyber Threat Landscape: The Hacker’s Perspective,” Centre for Secure Information Technologies, World Cyber Security Technology Research Summit – Belfast, Ireland, May 2017
- Moderator, Implementing the New DFS Cybersecurity Regulation, Cardozo Law School – New York, NY, April 2017
- Speaker, “Making the Case: Presenting Cyber Evidence Persuasively,” In-Q-Tel Cyber Sensemaking Forum – Virginia, January 2016
- Speaker, “Managing Cyber Risk and Its Effect on Business,” The Contingency Planning Exchange, New York Chapter Conference: Navigating the Emerging Risk Landscape – New York, NY, December 2016
- Keynote Speaker, “Cybersecurity: Threats, Consequences and Solutions,” McGuireWoods Data

Privacy Conference – Chicago, IL, November 2016

- Panelist, "Law Firms, Ethics & Cybersecurity," Practicing Law Institute – New York, NY July 2016
- Speaker, "Cybersecurity and Identity Theft Concerns for Banks," Florida International Bankers Association Cuba Workshop: How to Bank with Cuba – Havana, Cuba, July 2016.
- Lecturer, "Microsoft's Challenge to the Compelled Disclosure of Overseas Content Under the Stored Communications Act," Fordham University School of Law – New York, NY, April 2016
- Panelist, "Data Privacy and Cybersecurity: A New Legal and Enforcement Landscape," University of Chicago Law School – Chicago, IL, April 2016
- Moderator, "Setting Data Security Standards," Cardozo Law School – New York, NY, April 2016
- Panelist, "A World of Disruptive Innovations: Workable Solutions to Data Privacy and Public Policy Issues in the Sharing Economy," New York University Law School – New York, NY, February 2016
- Panelist, "Preparing for the Inevitable: A Cybersecurity Primer for the Futures and Derivatives Industry," Chicago Bar Association – Chicago, IL, January 2016
- Panelist, "Mitigating Catastrophe: Creating a Culture of Security," Northern District of Alabama 2015 Cybersecurity Summit – Huntsville, AL, September 2015
- Panelist, "Cyber Security: The Cold, Hard Reality of Protecting Financial Information," ABA Business Law Section Spring Meeting – San Francisco, CA, April 2015
- Lecturer, "Cyber Risk: The Need for a Comprehensive Approach," Rensselaer Polytechnic Institute – Troy, NY, March 2015
- Panelist, "Cyber-Crime – Security Threat: The Danger to Constitutional Rights and Human Privacy: The Future of the Law," Cardozo Law School – New York, NY, January 2015
- Faculty, "Avoiding Corporate Theft – Best Practices," 2015 DRI Corporate Counsel Roundtable – New York, NY, January 2015
- Speaker, "Cyber Warfare? Activism, Hack-tivism, & State Sponsored Attacks," Information Law & Policy Roundtable, Fordham University – New York, NY, January 2015
- Speaker, "Cyber Risk: Crossing the Government/Corporate Divide," International Conference on Cyber Security, Federal Bureau of Investigation/Fordham University– New York, NY, January 2015
- Speaker, "Protecting Our Digital Lives: New Challenges for Attorneys General," National Association of Attorneys General Winter Meeting – Ft. Lauderdale, FL, December 2014
- Panelist, "Managing Third Party Risks," NYSE Governance Services Forum – Washington, D.C., December 2014
- Panelist, "Cybersecurity and Disclosure Obligations," Ninth Annual National Institute on Securities Fraud, American Bar Association – New Orleans, LA, November 2014
- Panelist, "Cybersecurity: Mitigating Your Vulnerabilities," General Counsel Forum 2014 – New York, NY November 2014
- Speaker, "Dark Synergy: Hacktivists and Online Anonymity," The Risk and Security Management

Forum – Chichester, UK, October 2014

- Speaker, "Cyber Risk: Why Companies Need to Take a Comprehensive Approach," Loeb & Loeb 7th Annual IP/Entertainment Law Conference – Los Angeles, CA, September 2014
- Panelist, "Protecting Your Company: Managing Cybersecurity Risk," Simpson Thacher 2014 Corporate Counsel Leadership Conference – New York, NY, September 2014
- Panelist, "If You Have Nothing to Hide, You Have No Problem . . . Really? Evolving Expectations and New Realities When It Comes to Privacy," Missouri Bar Association – Kansas City, KS, September 2014
- Speaker, "Cyber Security," CFO Roundtable, Association of Management Consulting Firms – New York, NY, September 2014
- Panelist, "Cybersecurity and Data Privacy Trends," Clifford Chance Annual International Regulatory Conference – New York, NY May 2014
- Speaker, "The Dark Web and Silk Road: Online Anonymity and Bitcoins," RSA Conference 2014 – San Francisco, CA, February 2014
- Speaker, "The New Front Line is Online: Are Your Defenses Ready?" New York City Bar Association – New York, NY, October 2013
- Panelist, "The Interface of Technology & White Collar Crime," West LegalEdcenter Program – New York, NY, October 2013
- Faculty, "Cybersecurity 2013: Managing the Risk," Practicing Law Institute – New York, NY, July 2013
- Speaker, "U.S. Cybercrime 2013: Today's Stark Realities," Yale Club – New York, NY, June 2013
- Panelist, "The Shared Challenge of Cybersecurity," Financial Regulation and Enforcement Symposium 2013 – New York, NY, May 2013
- Faculty, "Investigating 'the Cloud'," National Advocacy Center, United States Department of Justice – Columbia, SC, April 2013
- Faculty, "Getting Targets and Electronic Evidence from Foreign Countries," National Advocacy Center, United States Department of Justice – Columbia, SC, April 2013
- Faculty, "Cybercrime: A Multi-Faceted Legal Challenge," Practicing Law Institute – New York, NY, April 2013
- Speaker, "Cyber Crime and Other Economic Crimes," Dallas Bar Association – Dallas, TX, March 2013
- Panelist, "New Faces of Economic Crime," University Club – New York, NY, February 2013
- Panelist, "Cyber-Rights and Cyber-Wrongs: Emerging Issues in Cybercrime Enforcement and Implications for the Future," New York State Bar Association – New York, NY, February 2013
- Faculty, "Cyber Theft and Other Data Protection Concerns," Practicing Law Institute's Corporate Counsel Institute 2012 – New York, NY, October 2012

- Panelist, “Cybercrime and National Security,” Concordia Summit – New York, NY, September 2012
- Lecture to Federal Security Service of the Russian Federation: “Presenting Cyber Cases to Juries” – Washington, DC, July 2012
- Faculty, Department of Housing and Urban Development, In-Service Training – New York, NY, July 2012
- Panelist, American Bar Association’s Criminal Justice Section’s Third Annual Prescription for Criminal Justice Forensics – New York, NY, June 2012
- Faculty, “Recent Hacktivist Prosecutions,” National Advocacy Center, United States Department of Justice – Columbia, SC, May 2012
- Panelist, “The New Faces of Crime, Cyber Crime: Greater Risks, Data Breaches, Hacking, Trade Secrets, Confidentiality,” Harvard Club – New York, NY, January 2012
- Speaker, “Prosecuting Overseas Cyber Criminals,” International Conference on Cyber Security, Federal Bureau of Investigation/Fordham University – New York, NY, January 2012
- Speaker, “Overview of Operation in Our Sites,” National Intellectual Property Rights Center Symposium: Online IP Theft in the 21st Century – Washington, DC, September 2011
- Keynote Speaker, Cyber Infrastructure Protection Conference 2011, City College of New York – New York, New York, July 2011
- Speaker, 5th Anti-Counterfeiting & Brand Protection Summit – New York, NY, September 2010
- Speaker and Law Enforcement Workshop Panelist, International Conference on Cyber Security, Federal Bureau of Investigation/Fordham University – New York, NY, August 2010
- Panelist, Arnold & Porter LLP In-House Seminar, “Brand Integrity, Security, and Anti-Counterfeiting for the Pharmaceutical Industry” – New York, NY, June 2010
- Faculty, Practicing Law Institute, New York and New Jersey Intellectual Property Rights Conference – New York, NY, November 2009
- Faculty, “CAN-SPAM Act Prosecutions,” National Advocacy Center, United States Department of Justice – Columbia, SC, June 2008
- Faculty, “Tracking Cell Phones: The Law, the Technology and Proposed Legislation,” National Advocacy Center, United States Department of Justice – Columbia, SC, June 2007