Lawyers

Nicole Friedlander

Partner

New York
T. +1-212-558-4332
F. +1-212-558-3588

friedlandern@sullcrom.com

PRACTICES & CAPABILITIES

Corporate Culture, Workplace Investigations & Whistleblower Litigation

Criminal Defense & Investigations

Cybersecurity

Digital Assets

FCPA & Anti-Corruption

Privacy

Securities & Commodities Investigations & Enforcement Practice

EDUCATION

2001, New York University School of Law, J.D.

1998, University of Pennsylvania, B.A.

BAR ADMISSIONS

New York

Nicole Friedlander is a partner in Sullivan & Cromwell's Criminal Defense and Investigations Group and co-head of its Cybersecurity Practice. Ms. Friedlander represents clients in complex internal investigations, regulatory enforcement proceedings and criminal matters involving every aspect of white-collar crime, including fraud, FCPA, insider trading, theft of trade secrets, money laundering and tax matters. Ms. Friedlander also advises major corporations and Boards of Directors in cybersecurity planning and incident response. She currently serves as co-chair of the New York Chapter of the Women's White Collar Defense Association and as a member of the New York City Bar Association's White Collar Crime Committee. Ms. Friedlander has been ranked by *Chambers USA* 2021 for White-Collar Crime & Government Investigations, where sources praised her "impress[ive] facility and judgment," her ability to "quietly command[] the room with her skilled preparation," and her standout trial skills ("She is so good in court.").

Ms. Friedlander joined the Firm in 2016 from the United States Attorney's Office for the Southern District of New York, where she was Chief of the Complex Frauds and Cybercrime Unit, and served for over eight years. In white-collar, among a wide range of cases, Ms. Friedlander led major prosecutions of offshore banks for facilitating tax evasion; secured one of the largest-ever FCPA resolutions; led cutting edge prosecutions of virtual currency exchangers for money laundering and Bank Secrecy Act violations; and brought a groundbreaking racketeering case against the owner of multibillion-dollar payday lending companies. In cybersecurity, Ms. Friedlander led the successful investigation of the largest-ever cyber theft of customer data from a U.S. financial institution; oversaw the indictment of Iranian state-sponsored hackers for coordinating cyberattacks on 46 financial institutions; and prosecuted a Russian national for hacking U.S. banks in a case the FBI named one of its top ten of the year. Ms. Friedlander was also a part of the litigation team that challenged an internet services provider to comply with a warrant, leading to Congress' passage of the CLOUD Act.

During her tenure at the U.S. Attorney's Office, Ms. Friedlander also successfully tried numerous federal criminal cases and briefed and argued appeals before the U.S. Court of Appeals for the Second Circuit.

Selected Rankings and Recognitions

- Recognized as a leader by *Chambers USA* in White-Collar Crime

& Government Investigations (2021)
- Named to Cybersecurity Docket's "Incident Response 30" (2019) and "Incident Response 40" (2021-2022)
- Named to *Global Investigations Review*'s Top 100 Women in Investigations worldwide (2018)
- Named a Rising Star by *The New York Law Journal* (2016)
- Recipient of National Association of Former U.S. Attorneys' Exceptional Service Award (2015)
- Recipient of Federal Executive Board's Distinguished Teamwork Award (2013)
- Named Federal Law Enforcement Foundation's "Prosecutor of the Year" (2012)

Recent Speaking Engagements and Events

- "Doing Business in and with China" (PLI, December 6, 2021)
- "Information Security" (ABA's 36th Annual National Institute on White Collar Crime, October 27, 2021)
- "Bank Boards of Directors Key Risks and Responsibilities in 2021: Actions Counsel Should Take Now" (webinar hosted by Strafford, August 17, 2021)
- "Ransomware Attacks" and "Breaches in the M&A Context and Disclosure Controls in Cybersecurity" (as co-moderator at Sandpiper Partners' third annual Cybersecurity and Privacy East Coast Conference, July 23, 2021)
- "Cybersecurity Update" (SIFMA C&L Society's Virtual Forum 2021, July 20, 2021)
- "FCPA, Sanctions and Anti-Money Laundering" (PLI's Doing Business in and with Emerging Markets 2021, June 7, 2021)
- "Working With the Regulator" (*Journal of Law and Cyber Warfare* Conference, November 19, 2020)
- "Secrets Protection, Enforcement, and Litigation" (Sandpiper Partners webinar, November 17, 2020)
- "Confronting Cybersecurity and Data Privacy Challenges in Times of Unprecedented Change" (New York University School of Law's Program on Corporate Compliance and Enforcement, October 14, 2020)
- "Cross-Border Regulatory and Enforcement Perspectives" (Sandpiper Partners Modernization of Canadian Privacy and Cybersecurity Framework conference, October 1, 2020)
- "The Global Threat of Cyberwarfare: From Work at Home to Infrastructure and Election Insecurity" (WomenCorporateDirectors 2020 Virtual Global Institute, September 9, 2020)
- "Cybersecurity Guidelines for Regulatory Agencies" (Thomson Reuters the Global Cyber Institute webinar, July 14, 2020)
- "FCPA, Sanctions and Anti-Money Laundering" (PLI's Doing Business in and with Emerging Markets 2020, June 1, 2020)

SELECTED REPRESENTATIONS

White-Collar

- Represented Goldman Sachs in reaching coordinated resolutions in multiple criminal and regulatory investigations in jurisdictions around the world relating to an alleged multi-billion dollar money laundering and corruption scheme involving the Malaysia sovereign development company, 1MDB, and senior public officials in Malaysia and the United Arab Emirates, including a deferred prosecution agreement with the DOJ and resolutions with the government of Malaysia, the SEC, Federal Reserve, New York DFS, and regulators in the UK, Hong Kong and Singapore.
- Represented Wells Fargo in resolving multiple criminal and regulatory investigations, including by the DOJ, the SEC and a multi-state working group of attorneys general, as well as in civil litigation, related to Wells Fargo's sales practices.
- Represents a U.S. financial institution in DOJ, bank regulatory and internal investigations into potential AML and Bank Secrecy Act violations arising from payments that flowed through the bank in connection with the FIFA and Petrobras bribery schemes.
- Represents a global financial institution in DOJ and bank regulatory investigations into billions of dollars in payments processed in violation of U.S. sanctions laws.
- Conducted an internal investigation for a multinational company concerning price-fixing in a U.S. auction market.
- Conducted an internal investigation for a multinational company concerning potential cross-border tax violations and tax evasion.
- Represented senior executives of a global financial institution in a bank regulatory investigation concerning potential diligence and oversight failures regarding problematic transactions. The regulator declined to take action against them.

Cybersecurity

- Represented a technology company in responding to the cyber theft of its source code, including notification to millions of customers, coordination with law enforcement, and conducting an internal investigation.
- Advised numerous companies and individuals victimized in cyber-fraud and phishing schemes, including coordination with federal and international law enforcement and of overseas litigation resulting in substantial recoveries for our clients. We have secured substantial and complete recoveries for clients, and recovered millions of dollars on numerous occasions. In one instance, as a result of our work, our client recovered almost the entirety of more than $20 million diverted by cybercriminals to Hong Kong.
- Advised a public technology company that received ransom demands to prevent hackers from publicly disclosing stolen company data, and lead the investigation into the theft of that data.

Attorney Advertising • Prior results do not guarantee a similar outcome.

- Represented numerous public companies in responding to ransomware attacks and cyber extortion schemes.
- Represented Popular in responding to a criminal cyber breach of company systems, including on state privacy issues, nationwide customer notification, and coordinating with their prudential banking regulator.
- Represented Scottrade with respect to the exposure of unencrypted files containing customers' personal data, including on state privacy law issues and nationwide customer notification.
- Advised multiple acquirers, and their financial advisors, engaging in M&A transactions in which significant data breaches were discovered at the target within days or hours of closing. All deals were successfully completed.
- Advised a public company regarding a potential breach of its network by a hostile nation-state, including coordinating with federal law enforcement and intelligence agencies.
- Advised a major technology company in connection with a forensic investigation of an employee suspected of stealing sensitive data and intellectual property worth billions of dollars.
- Represented a public company in an SEC investigation concerning a potential data breach.
- Advised a public company that was targeted in "brute force" cyber attacks by a party seeking to obtain information for its advantage in potential litigation, as a result of which the party abandoned the threatened litigation.
- Represented a financial institution in an investigation and in responding to an inquiry by the New York DFS and foreign law enforcement regarding a cybersecurity breach at a client that resulted in the loss of millions of dollars in customer funds.
- Advised a major real estate company and commercial landlord on the legal and regulatory implications of the installation of thermometer readers in commercial lobbies across multiple states in response to COVID-19.
- Advised a public company retailer regarding a potential cybercriminal compromise of its payment processing platform resulting in unauthorized charges on customers' credit cards.
- Advising a retailer in connection with a cybersecurity breach at its third-party e-commerce platform.
- Advised a global financial services firm that lost funds to criminals overseas in a cyber-fraud scheme, including working with U.S. and foreign law enforcement, and tracing and instituting actions to freeze and recover the stolen funds. We successfully recovered millions of dollars for our client in weeks.
- Advised and assisted over a dozen public companies in responding to SEC requests concerning the SolarWinds breach and other compromises.
- Advises regional, national and international financial institutions, and public and private corporations across industries on cyber

governance responsibilities, including advice to boards of directors and senior management on incident response planning, disclosure controls and procedures, director duties related to cybersecurity risks, and the coordination and implementation of cybersecurity "tabletop exercises."

- Advising the Bank Policy Institute, a consortium of the nation's leading banks, on the legal and regulatory implications of paying or facilitating the payment of ransom in response to ransomware attacks.
- On behalf of the Bank Policy Institute, SIFMA, the American Bankers' Association and the International Bankers' Association, drafted a joint trade associations' comment letter, on behalf of hundreds of financial institutions, regarding the notice of proposed rulemaking by the federal bank regulators concerning computer security incident notification requirements.
- Regularly advises certain major financial institutions on the legality and legal risks associated with particular transfers they are asked to make for customers to facilitate the purchase of cryptocurrency to pay ransom. Advises on OFAC and FinCEN requirements (including MSB and SAR-filing issues).
- Represents numerous financial institutions, hedge funds and global companies as standing outside cyber counsel.

Attorney Advertising • Prior results do not guarantee a similar outcome.