



# Data Strategy & Security

# Introduction

## Data is one of companies' most valuable assets and greatest risks.

The global flow of information creates constantly changing challenges: How do companies acquire, store, protect, use, and share data to keep up with the competition while reducing their legal and reputational risks?

Companies need an experienced and creative partner to help them design and execute their overall data strategy, whether they are:

- Building or revising data governance and board oversight programs;
- Developing artificial intelligence or big data programs;
- Conducting cyber and data-related due diligence in mergers, acquisitions, and other transactions;
- Enhancing cybersecurity preparedness and enterprise resilience;
- Addressing insider risk and protecting sensitive or proprietary information;
- Responding to ransomware attacks, data breaches, or other cyber incidents;
- Conducting internal or regulatory investigations involving data privacy, cybersecurity, or AI; or
- Defending against data privacy, cybersecurity, or AI-related litigation.

“I view them as some of the best in the industry; they are knowledgeable, thought leaders in this space with tremendous amounts of experience. They are leading issues impacting the cyber industry.”

“The team has a very strong understanding of regulatory impact and the bench is second to none.”

*Chambers USA, 2025*

---

Ranked as a leading firm for Cyber Law (including Data Privacy & Data Protection).

“The expertise of the lawyers at Debevoise is unmatched. They have some of the most experienced lawyers in the trade.”

“The team’s breadth of knowledge stands out; I would consider them not just practitioners, but experts in the field.”

*The Legal 500 US, 2025*

---

**Winner** of two *Financial Times* North America Innovative Lawyers Awards:

“Innovation in New Legal Products” (2025) for our STAAR platform and

“Innovation in Digitizing Legal Services” (2022) for our cybersecurity Data Portal.

## Data Strategy & Security Services

The Debevoise Data Strategy & Security (DSS) practice is global and interdisciplinary—combining our cybersecurity, privacy, artificial intelligence, business continuity, M&A diligence, and data governance practices into one fully integrated and coordinated group.

Our calling card has been our ability to skillfully resolve the most complex, high-stakes, technical cyber incidents, including working in the classified space and with law enforcement, where sophisticated clients routinely tell us that our connections and experience are unmatched.

Our cyber incidents work is just one part of our matrix. We leverage our leadership's experience as DOJ and SEC attorneys to lead internal and whistleblower investigations related to cybersecurity regulatory compliance, conduct cybersecurity risk assessments, make board presentations, and litigate data breach and business-email compromise cases. Additionally, as cyber and AI rapidly converge, Debevoise stands out as one of the only firms where leading cybersecurity and AI practices are fully integrated (our DSS practice co-leaders are ranked by *Chambers USA* as Band 1 for Privacy & Data Security and Band 1 for AI, respectively).

Combined with our robust privacy and national security capabilities, we are perfectly positioned to deliver nuanced, practical advice to clients on the novel and cutting-edge data and information security issues presented by emerging AI use cases and multinational business operations. This includes advising clients on the use of sensitive or commercially valuable IP with AI systems, sharing such data with third-party AI service providers, and compliance with the DOJ's bulk data transfer rule. Complementing our advisory work in the cyber, privacy and AI space is a team of practitioners well versed in cyber-adjacent transactional, regulatory and SEC matters. Our growing cyber and privacy litigation practice has made tremendous strides in the past year, adding more complex litigation defense on behalf of our clients. Along with members of our White Collar practice, we are also increasingly advising clients on insider risk issues.



Among the factors that set us apart from other groups:

- We are recognized by *Chambers USA* for both Cybersecurity and AI, and our practice co-leaders are ranked Band 1 in Cybersecurity and AI, respectively. We are also the only group with a cybersecurity attorney ranked Band 1 in *Chambers* for Crisis Management, and we are the only group with five attorneys ranked for Cybersecurity.
- We have three partners featured on *Cybersecurity Docket's* 2025 "Incident Response 50 List."
- Our AI practice is a dedicated team of several full-time AI lawyers, who are organized into specialized AI subject-matter teams and work closely with regulatory compliance experts in other practice groups who have the technical proficiency and government experience to help clients take a risk-based approach to applying existing laws to novel AI use cases and anticipate how new AI laws may be applied to our clients' use of AI.
- Debevoise's AI team has also developed an innovative, monthly subscription-based Suite of Tools for Assessing AI Risk (STAAR), which won the Financial Times Innovative Lawyers North America Award for Innovation in New Legal Products in 2025. STAAR brings together the firm's market-leading AI legal, regulatory, and governance expertise into a single, technology-enabled platform. The legal industry has recognized the STAAR platform as a visionary model for AI legal services in the Law.com article, "[Debevoise & Plimpton Is Building a New Model for Delivering AI Adoption Advice](#)," in the Law360 article, "[Debevoise Builds Tool To Help In-House Attys Assess AI Risk](#)" and most recently in *Legaltech News*. In March 2026, Debevoise launched STAAR 2.0, an enhanced version of its client facing AI platform. STAAR 2.0 is built with Legora's Portal architecture, which converts the knowledge gained from five years of advising over 100 clients on complex AI-related regulatory, compliance, and transactional matters into a practical, searchable workspace. STAAR 2.0 has been featured in numerous articles, including most recently the Law.com article "Debevoise Partners with Legora on 2nd Iteration of Subscription-Based AI Advisory Offering."
- Our attorneys have deep technical expertise and include lawyers with engineering degrees and other highly technical experience.
- Our practitioners also have in-house experience, including a former chief in-house counsel for cyber, privacy, and data work at a Fortune 50 company and numerous associates with secondment experience in-house.
- We have multiple former Assistant U.S. Attorneys who led cyber teams and global cyber investigations at the Department of Justice.
- Our partners have been appointed to the New York State Cybersecurity Advisory Board and New Jersey Supreme Court Committee on AI and the Courts.
- We have multiple partners with deep national security experience that enables them to assist clients on sensitive cybersecurity matters that intersect with national security.





“Their industry knowledge and experience make them suited to address complex, sophisticated matters. Regulatory compliance, litigation, emerging issues — they have resources to address all my needs.”

“Debevoise’s team possesses a deep understanding of the complex legal landscape, particularly when it comes to a risk specific to our business. Their insights have been invaluable.”

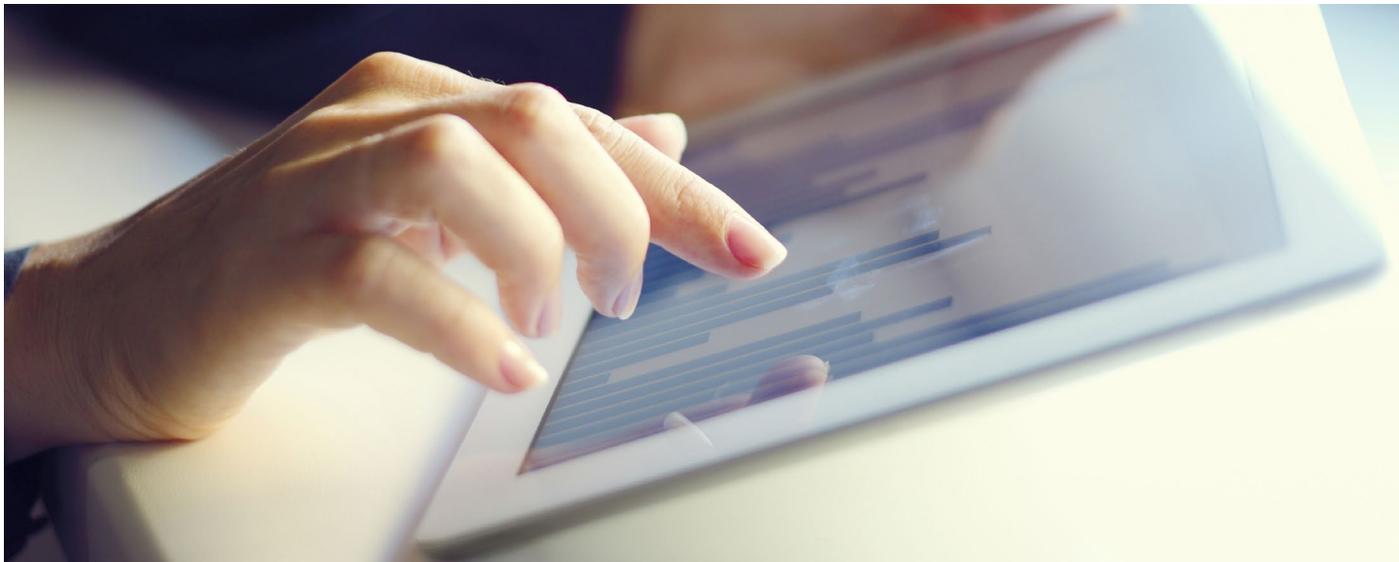
*Chambers USA, 2025*

## A FULL RANGE OF DATA GOVERNANCE, PROTECTION, AND PRIVACY SERVICES, INCLUDING CYBER INCIDENT RESPONSE AND MANAGING AI RISK

Our experience and advice covers the full spectrum of cyber threats (including from nation states, criminal ransomware groups, insiders, and critical vendors), as well as compliance with the ever-growing array of cybersecurity, privacy, and AI regulations in the U.S. and across the globe.

- **360° Incident Response Services.** Debevoise helps clients navigate cyber incidents with the full range of services, including immediate crisis management, internal and external communications, fact investigation, breach notification, regulator and law enforcement engagement, civil regulatory investigations, defense of class action and derivative litigation, and briefings to the board and C-Suite.
- **Engaging with Law Enforcement in the U.S. and Globally.** We are able to leverage our worldwide network of law enforcement contacts in the event of an incident. Our team includes several former federal cybercrime prosecutors, including the former leader of the Justice Department’s Criminal Division, the former leader of the Department’s response to national security cyber threats, and two other former Assistant U.S. Attorneys who brought landmark cyber cases in the country’s federal courts.
- **Review/Update Data Policies and Governance.** We can provide an assessment of the company’s policies and procedures for the protection and handling of consumer and employee personal data, as well as sensitive company information, with particular attention to mitigation of legal, business, and reputational risks.

- **Cyber-, Privacy-, and AI-Risk Assessment.** In today’s dynamic regulatory environment, managing risks at the intersection of law and technology means measuring data protection and data optimization strategies against existing laws and regulations, as well as anticipated changes in the legal and threat environments. We review companies’ cybersecurity, privacy, and AI programs and assess them against existing and emerging legal standards. Our work ranges from leading a full legal and technical risk assessment of various data programs, typically performed in tandem with a technical vendor, to a targeted review of areas known to attract regulatory and enforcement focus.
- **Board/Executive Briefings and Training.** We regularly brief boards and company executives on the latest threats their companies face relating to data in order to help them assess risk, allocate resources, maintain appropriate insurance, prevent avoidable losses, and discharge their oversight obligations. We also provide training on cybersecurity, privacy, and AI risks to new executives and board members, as well as anyone wishing to learn more about their responsibilities in these areas.



- **Realistic Tabletop Exercises.** We are known for running extremely realistic cyber incident simulations or “tabletops” to help our clients prepare for adverse cybersecurity, privacy and AI events by conducting real-world drills of actual data events for various functions within the organization including Legal, Compliance, IT, Risk, Communications, Executive Management, and the Board. These exercises, which regulators increasingly expect companies to conduct, allow our clients to test their incident response plans and see how their organization works through emergency data events, including ransomware attacks that shut down operations, insider data theft, whistleblower allegations of AI bias, state-sponsored hacking of sensitive commercial information, leaking of large volumes of customer or employee personal information, and compromise of a critical vendor’s information systems.

- **Vendor Risk Review.** Cyber incidents often involve exploitation of a vendor's trusted access to the company's systems, its handling of sensitive data on behalf of the company, or risks posed by the vendor as a single point of operational failure. Accordingly, regulators have honed in on this challenging area. We work with our clients to develop practical, risk-based strategies to manage third-party cyber, privacy, and AI risks through their policy development, diligence efforts, contractual terms, and insurance strategies.
- **M&A Due Diligence.** Data risks are increasingly prominent in M&A due diligence and in the post-acquisition integration process. We often lead cyber, privacy, and AI diligence investigations around the world, including advising on policies and procedures for due diligence and for integration generally, as well as on risks and issues raised by specific actual or potential acquisitions and investments.
- **Insurance.** Companies increasingly are concluding that cyber-, AI-, and privacy-specific insurance policies are essential. Our team has significant experience working inside the insurance industry and can review existing policies to assess coverages and exclusions.

## REAL-WORLD EXPERIENCE

Our services are based on experience in the trenches of many of the country's landmark cyber and privacy incidents (including many non-public incidents). Our lawyers have deep technical knowledge that allows them to translate complex technical findings into legal and business decision points. This has enabled us to provide a pragmatic approach to identifying and coordinating the key elements of effective incident response and overall data strategy.

Before joining Debevoise, partner Luke Dembosky served as Deputy Assistant Attorney General for National Security, managing the Justice Department's work on all national security cyber incidents, including the cyber attack on Sony Pictures and the landmark breaches of Target, The Home Depot, Anthem, and the U.S. Office of Personnel Management, among many others. At Debevoise, Luke co-chairs the Cyber and Privacy practice, acting for the firm's clients on high-profile and high-stakes global and U.S. breach matters.

# Our Team Leads

## U.S. & UK Team

### Luke Dembosky



Partner and Practice Leader, Washington, D.C. • [ldembosky@debevoise.com](mailto:ldembosky@debevoise.com) • +1 202 383 8020

Luke Dembosky Co-Chairs the firm's global Data Strategy & Security Group. He advises companies on managing cyber risks, responding to cyber incidents, and handling related internal investigations and regulatory defense. Luke is recognized by *Chambers* with a Band 1 ranking in Crisis Management, where he is the only cyber lawyer ranked in that category. He is also ranked Band 1 for Privacy and Data Security: Cybersecurity, and is recognized by *Cybersecurity Docket's* "Incident Response 50 List." He is regularly asked to speak to boards of directors and senior leadership teams on emerging cyber-related issues. Luke joined Debevoise in March 2016 after serving as Deputy Assistant Attorney General for National Security at the U.S. Department of Justice, where he oversaw all national security cyber matters for the agency. His 14 years at DOJ included serving as DOJ's representative at the U.S. Embassy in Moscow and as the senior DOJ official on the Target, Sony Pictures, Anthem, and OPM breaches, among many others.

### Avi Gesser



Partner and Practice Leader, New York • [agesser@debevoise.com](mailto:agesser@debevoise.com) • +1 212 909 6577

Avi Gesser is Co-Chair of the firm's Data Strategy & Security Group. His practice focuses on advising major companies on a wide range of cybersecurity, privacy, and artificial intelligence matters. He has represented global financial services firms, private equity firms, insurance companies, hedge funds, and media organizations in large-scale ransomware attacks, cyber breaches by nation-states, and regulatory investigations relating to the use of artificial intelligence. Mr. Gesser regularly advises boards and senior executives on governance, risk, and liability issues relating to cybersecurity and AI. Mr. Gesser is also a primary author of the firm's Data Blog and created the pioneering monthly subscription-based Suite of Tools for Assessing AI Risk (STAAR), which won the *Financial Times* Innovative Lawyers North America Award for Innovation in New Legal Products in 2025. STAAR brings together the firm's market-leading AI legal, regulatory, and governance expertise into a single, technology-enabled platform, which has been featured in numerous articles, including most recently in *Legaltch News*. He is ranked Band 1 by *Chambers USA* for Artificial Intelligence and in the highest category by *Chambers Global*. He is also recommended by *Chambers Global*, *Chambers USA*, and *The Legal 500* as a leading lawyer for privacy and data security.

### Erez Liebermann



Partner, New York • [eliebermann@debevoise.com](mailto:eliebermann@debevoise.com) • +1 212 909 6224

Erez Liebermann is Co-Chair of the firm's Technology Group and a core member of our Data Strategy & Security Group. His practice focuses on advising major businesses on a wide range of complex, high-impact cyber-incident response matters and on data-related regulatory requirements. With decades of experience in data issues as a litigator, federal prosecutor, and senior in-house counsel at a global insurance company, Mr. Liebermann regularly advises clients at the C-suite and board level on building strategies to reduce their data-related regulatory and reputational risks and on navigating high-profile government investigations following data incidents. He is also widely acknowledged as a leading cybersecurity and data privacy professional and is highly ranked among the leading lawyers by *Chambers Global*, *Chambers USA*, *Cybersecurity Docket's* "Incident Response 50 List," and *The Legal 500*. Clients note that he is "very talented" and "one of the most intelligent attorneys [and] very practical and great to work with."

## Robert Maddox



Partner, London • [rmaddox@debevoise.com](mailto:rmaddox@debevoise.com) • +44 20 7786 5407

Robert Maddox is a partner in the firm's Data Strategy & Security Group. In 2021, he was named to *Global Data Review's* "40 Under 40" and is described as "a rising star" in cyber law by *The Legal 500 US*. His practice focuses on cybersecurity incident preparation and response, internal investigations, and regulatory defense. Mr. Maddox also advises on data strategy and compliance in the context of emerging technologies, including AI, and operational resilience matters. He has been part of leading the response to some of the largest cyber incidents in Europe and frequently advises clients on DORA and NIS2 compliance. Mr. Maddox acts for clients across a wide range of industries including financial services, private equity, media, and entertainment, as well as for sovereign states and international organizations. He helps clients respond to all types of cybersecurity incidents, including APT/nation state threat actors, business email compromises, ransomware, and payment-skimming attacks.

## Charu Chandrasekhar



Partner, New York • [cchandra@debevoise.com](mailto:cchandra@debevoise.com) • +1 212 909 6774

Charu Chandrasekhar is a litigation partner based in the New York office and a member of the firm's Data Strategy & Security and White Collar & Regulatory Defense Groups. Charu has significant experience representing global financial institutions and public companies in a broad range of securities-related government investigations, examinations, and enforcement matters, with particular experience in cases involving artificial intelligence and cybersecurity. Charu also has substantial experience advising investment advisers, broker-dealers, and public companies on artificial intelligence and cybersecurity governance, policies, and procedures. She is a frequent contributor to the firm's Data Blog on AI regulatory and compliance issues impacting financial services firms and is a regular speaker on AI issues impacting SEC, CFTC, and FINRA registrants. She is ranked by *Chambers* for Securities: Regulation: Enforcement.

## Jim Pastore



Partner, New York • [jjpastore@debevoise.com](mailto:jjpastore@debevoise.com) • +1 212 909 6793

Jim Pastore is a litigation partner and a member of the firm's Data Strategy & Security Group and Intellectual Property Litigation Group. His practice focuses on privacy and cybersecurity issues. Mr. Pastore is recognized by *Chambers USA* and *The Legal 500 US* for his cybersecurity work and was included in *Benchmark Litigation's* "Under 40 Hot List," which recognizes attorneys under 40 with outstanding career accomplishments. Mr. Pastore has also been named six consecutive times to *Cybersecurity Docket's* "Incident Response 50," a list of the best and brightest data breach response attorneys. Prior to rejoining Debevoise in 2014, Mr. Pastore served for five years as an Assistant United States Attorney in the Southern District of New York, where he spent most of his time as a prosecutor with the Complex Frauds Unit and Computer Hacking and Intellectual Property Section.

## Matthew Kelly



Counsel, New York • [makelly@debevoise.com](mailto:makelly@debevoise.com) • +1 212 909 6990

Matthew Kelly is a counsel and a member of the Data Strategy & Security Group. His practice focuses on advising the firm's growing number of clients on matters related to AI governance, compliance, and risk management, and on data privacy. Mr. Kelly has extensive experience advising public companies and companies across the financial services sector, on internal investigations and regulatory matters involving data strategy, governance, and compliance. He has advised clients on the usage of quantitative modeling tools and data-driven operations and on the design and implementation of post-Dodd-Frank model governance frameworks. Mr. Kelly has also led multiple advisory and regulatory matters related to algorithmic trading and data governance for broker-dealer and investment advisory clients, including SEC, FINRA, and New York Attorney General investigations. Mr. Kelly is ranked as "Up and Coming" by *Chambers* for Privacy and Data Security and is recognized by *The Legal 500 US* for Cyber Law.

## Johanna Skrzypczyk

Counsel, New York • [jnskrzypczyk@debevoise.com](mailto:jnskrzypczyk@debevoise.com) • +1 212 909 6291



Johanna Skrzypczyk is a counsel in the Data Strategy and Security practice of Debevoise & Plimpton LLP. Her practice focuses on advising on AI matters and privacy-oriented work, particularly related to the California Consumer Privacy Act. Prior to joining Debevoise, Ms. Skrzypczyk served as Assistant Attorney General in the Bureau of Internet and Technology at the New York Attorney General's Office. In this role, she helped draft the amendments to New York's data breach law (known as the SHIELD Act); investigated, litigated, and negotiated the landmark settlement of an action against a national corporation regarding credential stuffing, one of the very few regulatory actions to address this widespread type of cyberattack; and co-lead an initiative involving potential discriminatory impacts of AI. Ms. Skrzypczyk also worked on matters involving consumer privacy, data security and virtual markets. Ms. Skrzypczyk was recognized by *The Legal 500 US* in the Cyber Law category.

---

## Carter Burwell

Partner, Washington, D.C. • [cburwell@debevoise.com](mailto:cburwell@debevoise.com) • +1 202 383 8149



Carter Burwell is a litigation partner based in the Washington, D.C. office and a member of the firm's White Collar & Regulatory Defense practice. His practice focuses on white collar criminal defense, government and internal investigations, and national security. He has represented some of the world's largest technology companies in high-stakes global matters. His work tends to involve high-profile controversies tied to current events, ongoing political disputes, and underlying and competing policy interests. He joined Debevoise in 2021 after more than a decade in senior roles across the federal government. Carter served as Counselor to the Secretary of the Treasury for Terrorism and Finance Intelligence, where he advised on national security matters. Prior to his role at the Treasury Department, he served as one of the top lawyers on the U.S. Senate Judiciary Committee, including as Chief Counsel to former Assistant Majority Leader and U.S. Senator John Cornyn and as Counsel to former Chairman and U.S. Senator Chuck Grassley. Carter also served as an Assistant U.S. Attorney in the Violent Crime and Terrorism Unit in the U.S. Attorney's Office in the Eastern District of New York (EDNY) and in the National Security and International Crimes Unit in the U.S. Attorney's Office in the Eastern District of Virginia (EDVA).

---

## Daniel Gitner

Partner, New York • [dmgitner@debevoise.com](mailto:dmgitner@debevoise.com) • +1 212 909 6898



Daniel Gitner is a partner in the White Collar & Regulatory Defense Group. He focuses his practice on advising corporations and institutions on a broad range of white collar matters, especially those involving complex, large-scale crises and government investigations. He also currently advises companies with respect to cybersecurity issues, including matters currently being investigated by the DOJ Civil Cyber Fraud Initiative. He is a Fellow of the American College of Trial Lawyers. Prior to joining the firm and from 2021 to 2025, he served as Chief of the Criminal Division for the United States Attorney's Office in the Southern District of New York. There, he oversaw all criminal investigations and prosecutions, including those involving cybercrime, securities and commodities fraud, market manipulation, insider trading, corporate fraud, sanctions, national security, foreign corrupt practices, public corruption, criminal tax, money laundering, the Bank Secrecy Act, civil rights, narcotics trafficking, and violent crime. He supervised a team of over 175 attorneys, investigators, and staff and regularly coordinated with leadership at other components of the Department of Justice and various federal and state law enforcement and regulatory agencies.

---

## Henry Lebowitz

Partner, New York • [hlebowitz@debevoise.com](mailto:hlebowitz@debevoise.com) • +1 212 909 6588



Henry Lebowitz is a corporate partner and a member of the firm's Data Strategy & Security and Intellectual Property Groups. His practice focuses on leading the IP and technology aspects of mergers and acquisitions, financings, capital markets, and other corporate transactions. Henry has early career background as a patent examiner in the U.S. Patent and Trademark Office, examining patent applications in the fields of digital error correction, computer reliability, and business methods and systems.

## Benjamin Pedersen



Partner, New York • [brpedersen@debevoise.com](mailto:brpedersen@debevoise.com) • +1 212 909 6121

Benjamin Pedersen is a partner in the firm's Capital Markets Group and a member of the Special Situations team. His practice focuses on a broad range of capital markets transactions, regularly advising public and private companies on securities laws, disclosure, corporate governance, and general corporate matters. Ben regularly advises clients on SEC cyber rule compliance and disclosure matters. Ben is ranked "Up and Coming" by *Chambers* for Capital Marketings: Debt & Equity. He is also recommended for debt and equity capital markets in *The Legal 500 US* (2025).

---

## Kristin Snyder



Partner, San Francisco • [kasnyder@debevoise.com](mailto:kasnyder@debevoise.com) • +1 415 738 5718

Kristin Snyder is a litigation partner and member of the firm's White Collar & Regulatory Defense Group. Her practice focuses on securities-related cybersecurity, regulatory, and enforcement matters, particularly for private investment firms and other asset managers. Ms. Snyder is recommended by *The Legal 500 US*. Prior to her role at Debevoise, Ms. Snyder served at the U.S. Securities & Exchange Commission (SEC) for 18 years, most recently serving as the Deputy Director of the Division of Examinations resident in its San Francisco Regional Office. In her role, she spearheaded the development of examination priorities for the national and international examination programs covering a spectrum of SEC registrants including investment advisers, investment companies, and broker-dealers.

---

## David Sarratt



Partner, San Francisco • [dsarratt@debevoise.com](mailto:dsarratt@debevoise.com) • +1 415 738 5701

David Sarratt is a partner in the firm's Litigation Department. He is a seasoned trial lawyer whose practice focuses on government enforcement actions, internal investigations, and complex civil litigation for financial institutions and other clients. Mr. Sarratt has particular experience in matters relating to compliance with the Bank Secrecy Act and the Foreign Corrupt Practices Act, as well as with novel enforcement issues arising from new technologies.

---

## Douglas Zolkind



Partner, New York • [dzolkind@debevoise.com](mailto:dzolkind@debevoise.com) • +1 212 909 6804

Douglas Zolkind is a litigation partner and a member of the firm's White Collar & Regulatory Defense Group. A former federal prosecutor with extensive trial experience, he defends corporate and individual clients in criminal and regulatory enforcement matters around the world. Douglas has extensive experience representing companies, boards, private equity firms, venture capital firms, financial institutions, digital asset firms, and individual executives in significant government investigations, enforcement matters, and internal investigations. He frequently defends clients before the Department of Justice, SEC, and state authorities and handles matters involving allegations of securities and commodities fraud, money laundering, violations of the Foreign Corrupt Practices Act (FCPA), U.S. sanctions, the Bank Secrecy Act, the False Claims Act, and cryptocurrency fraud and regulatory violations. For example, he is currently representing a global, public company in a cybersecurity matter being investigated by the Department of Justice. He has an international practice, often advising on cross-border investigations involving authorities in multiple jurisdictions. Prior to joining Debevoise, he served as an Assistant United States Attorney in the Criminal Division of the U.S. Attorney's Office for the Southern District of New York.

## Kim Le



Counsel, San Francisco • [kle@debevoise.com](mailto:kle@debevoise.com) • +1 415 738 5706

Kim Le is a corporate counsel and a member of the firm's Healthcare & Life Sciences Group. She is also active in the firm's Data Strategy & Security practice. As a leading practitioner on privacy, data security, and cyber-security issues, Ms. Le provides expertise in data breach reporting, including covered entity and business associate obligations under the HIPAA breach notification rule and audit response. Further, Ms. Le counsels clients regarding privacy and security preparedness, routinely redesigning compliance programs for provider organizations, hybrid entities, service vendors, and technology companies to improve operational effectiveness and decrease compliance risk.

---

## Anna Moody



Counsel, Washington, D.C. • [amoody@debevoise.com](mailto:amoody@debevoise.com) • +1 202 383 8017

Anna Moody is a counsel in Debevoise's Litigation Department, resident in the Washington, D.C. office. Her practice focuses on securities-related enforcement defense, including cybersecurity regulatory counseling and defense, SEC examinations, internal investigations, and white collar criminal defense. Anna represents individuals, private firms, and public companies in SEC and DOJ investigations and internal investigations. She advises on a variety of regulatory and enforcement issues, including with respect to cybersecurity and chief information security officer liability. She regularly counsels financial institutions in high-stakes insider trading investigations and advises on information barriers and related compliance. In addition to her regulatory defense work, Anna has represented corporate clients and their officers and directors in securities class actions and shareholder derivative litigation and has also successfully litigated significant cases in the appellate courts and the Supreme Court of the United States. She was a leading member of the Debevoise team that represents SolarWinds, a software developer, in an SEC investigation related to the December 2020 SUNBURST cyberattack.

## Europe | France

### Alexandre Bisch



Counsel, Paris • abisch@debevoise.com • +33 1 40 73 13 37

Alexandre Bisch is a counsel in the Paris office and a member of the firm's Litigation Department. Mr. Bisch focuses on white collar criminal defence and commercial litigation. He advises and represents companies and their executives in matters involving criminal, regulatory, and internal investigations. He also represents clients on a variety of civil and commercial disputes, including domestic and international litigations and enforcement of foreign judgments and arbitral awards.

## Asia | Shanghai

### Philip Rohlik



Counsel, Shanghai • prohlik@debevoise.com • +86 21 5047 0788

Philip Rohlik is a member of the firm's Litigation Group and leads the firm's dispute resolution team in Shanghai. His practice focuses on international investigations, securities law, and dispute resolution. It has included representation of U.S. and multinational companies in complex litigation and investigations, with a particular focus on Asia, including regularly counseling clients on relevant data protection and networks securities regulations in China. Mr. Rohlik also regularly advises corporate clients on regulatory issues arising in the course of their business around the globe or in connection with M&A transactions. Mr. Rohlik is admitted to practice law in New York and the United States District Court for the Southern District of New York and is a solicitor admitted to appear before the High Court of Hong Kong.

**New York**

66 Hudson Boulevard  
New York, NY 10001  
Tel: +1 212 909 6000  
Fax: +1 212 909 6836

**Washington, D.C.**

801 Pennsylvania Avenue N.W.  
Washington, D.C. 20004  
Tel: +1 202 383 8000  
Fax: +1 202 383 8118

**San Francisco**

650 California St  
San Francisco, CA 94108  
Tel: +1 415-738-5700  
Fax: +1 415 644 5628

**London**

The Northcliffe  
28 Tudor Street  
London  
EC4Y 0AY  
Tel: +44 20 7786 9000  
Fax: +44 20 7588 4180

**Paris**

103 rue de Grenelle  
75007 Paris  
Tel: +33 1 40 73 12 12  
Fax: +33 1 47 20 50 82

**Frankfurt**

Taunustor 1 (TaunusTurm)  
60310 Frankfurt am Main  
Tel: +49 69 2097 5000  
Fax: +49 69 2097 5555

**Debevoise & Plimpton (Luxembourg) SCS**

*Inscrit au Barreau de Luxembourg*  
4a, rue Albert Borschette  
L-1246 Luxembourg  
+352 28 5795 33 00

**Hong Kong**

21/F AIA Central  
1 Connaught Road Central  
Hong Kong  
Tel: +852 2160 9800  
Fax: +852 2810 9828

**Shanghai**

13/F, Tower 1  
Jing'an Kerry Centre  
1515 Nanjing Road West  
Shanghai 200040  
Tel: +86 21 5047 1800  
Fax: +86 21 5047 1600

**debevoisedata.com**  
**privacy**  
**security**  
**protection**