ALSTON & BIRD



Kimberly Kiefer Peretti

Partner

+1 202 239 3720 | kimberly.peretti@alston.com
Washington, D.C. | The Atlantic Building, 950 F Street, NW | Washington, DC 20004

Related Services

Privacy, Cyber & Data Strategy ▪ White Collar, Government & Internal Investigations ▪ Payments & Fintech ▪ Privacy & Cybersecurity Litigation ▪ Alston & Bird Global Privacy & Security Network (ABPSN) ▪ Attorneys General & State Enforcement ▪ Connected & Autonomous Vehicles ▪ National Security & Digital Crimes ▪ Committee on Foreign Investment in the United States (CFIUS) ▪ Insurance ▪ Retail ▪ Food & Beverage ▪ Consumer Protection/FTC ▪ Cybersecurity & Risk Management ▪ Crisis & Data Breach Response ▪ European Privacy & Cybersecurity ▪ Privacy & Cyber Regulatory Enforcement ▪ Litigation ▪ Blockchain & Digital Assets ▪ HIPAA/Health Information Privacy, Security & Breach Response ▪ Ransomware Fusion Center

A former DOJ cybercrime prosecutor and former director of PwC's cyber forensics group, Kim delivers top of the line cyber risk management and information security counsel to her clients. As co-leader of our Privacy, Cyber & Data Strategy Team and National Security & Digital Crimes Team, Kim is recognized by select publications and is frequently quoted by the media.

Kim Peretti is nationally known for her expertise in cybersecurity, handling high-profile data breach response matters across a wide range of industries, including healthcare, manufacturing, insurance, financial services, and retail. She also advises companies on cyber regulatory investigations and board-level cyber risk oversight.

With over 25 years of experience as both an information security professional and attorney, Kim brings a unique perspective shaped by her roles as a former senior litigator in the U.S. Department of Justice's Computer Crime and Intellectual Property Section (CCIPS) and a director in PwC's forensic services practice. Her work included leading landmark cybercrime prosecutions and guiding forensic investigations of nation-state attacks on critical infrastructure.

Kim is consistently recognized by *Chambers USA* (Band 1), *Chambers Global* (Band 1), The Legal 500, *The Best Lawyers in America*®, Cybersecurity Docket, and BTI Consulting Group. She has been featured on CNN's *Declassified* and CNBC's *American Greed* for her role in the prosecution of the global carding organization Shadowcrew and the infamous TJX hacker.

She is a Certified Information Systems Security Professional (CISSP) and holds the NACD Certificate in Cybersecurity Oversight. Demonstrating her commitment to advancing the field of cybersecurity, she co-founded Alston & Bird's Women in Cyber Network™ and served on the U.S. Secret Service's Cyber Investigation Board. In 2025, she launched the Ransomware Fusion Center to help organizations prepare for and respond to ransomware threats.

Representative Experience

Security Incident Response

- Represented a health care client involved in a ransomware attack, requiring both a complex forensic investigation and extensive data review and restoration processes.

- Represented a global company in connection with a network and cloud service provider attack by multiple state-sponsored actors targeting the infrastructure for both espionage and financial crime-based purposes. The response included extensive forensic investigation and data analytics efforts to identify and report on impacted information affecting both individuals and companies as well as working with national security and law enforcement arms of the U.S. government.
- Represented a global technology company in a targeted business email compromise scheme involving unauthorized wire transfers of multiple business partners over a several month period.
- Represented a health care client in an extensive cyber intrusion involving the collection of a large volume of data and provided advice on incident response, oversaw forensic investigators, and assisted with a large data review.
- Representing a large health care provider in a vendor website breach, including vandalism and attempted theft of databases with millions of PHI records compromised.
- Assisted one of the world's largest payment processors with investigation and notification in a security incident involving a subsidiary's e-commerce platform and payment card data. Our counsel included assistance with oversight of the forensic investigation, advising on issues related to investigation by the payment card brands, and individual and regulatory notifications in over 20 countries.
- Assisted a major financial services holding company in managing incident response, regulatory inquiries, and extensive cooperation efforts with the FBI for one of the top ten HIPAA breaches of 2018, resulting from social engineering and vishing attacks by foreign actors.
- Represented a large telecommunications company in investigating a sophisticated state-sponsored attack with national security implications, including facilitation of classified law enforcement interactions.
- Represented a large health care company in review and analysis of a ransomware incident involving an extensive and sophisticated intrusion.
- Represented a large international retail company with an incident involving cyber extortion of a subsidiary in connection with potential theft of personal data.
- Assisted a regional financial institution with hundreds of locations in analyzing breach notification and response obligations for skimming incidents.
- Assisted a community bank with investigation and response of incident involving placement of skimming device on ATMs.
- Represented several large global organizations in connection with government-led national security investigations resulting from state-sponsored attacks originating from different countries/threat actors.
- Represented a large, franchised restaurant business in connection with a cybersecurity incident investigation, including ongoing analysis of cybersecurity insurance issues, incident litigation, and regulatory defense.
- Represented one of the largest home improvement retailers in the U.S. in connection with a sophisticated cyberattack and criminal intrusion involving customized malware targeting payment card data from point-of-sale systems. The representation includes, among other areas, coordinating with the payment card brand networks and federal and state law enforcement agencies, directing the forensic investigation of the PFI and other third-party forensic firms, and defending multiple putative class actions filed by financial institutions.
- Represented a global diversified industrial company in connection with a targeted attack by sophisticated threat actors engaged in industrial espionage and financial fraud.

- Represented a global provider of business information in connection with a sophisticated intrusion by Eastern European organized criminal groups that impacted data breach laws and regulations in more than 50 countries. The incident response included directing a complex and technical forensic investigation involving U.S. and non-U.S. systems; analyzing U.S. state and federal and international breach notification statutes, regulations, and recommendations and coordinating the notification process; responding to numerous state attorneys general inquiries; development and execution of crisis communication plans; and participating in frequent senior executive and board-level meetings.
- Represented a global payment processor in connection with a technical, complex computer crime investigation involving a sophisticated cyber threat actor. The crisis response effort included advising on myriad legal issues, including securities law guidance, regulatory issues, class action defense, governmental investigations, and insurance coverage and issues. The effort also included supervising and managing a complex cyber forensic investigation that included a rapid response to a sophisticated intruder with deep and persistent access to the environment; development of containment, eradication, and remediation strategies; and coordination of the activities of multiple third parties, including an independent forensic investigator, several payment card brand networks, financial regulators, and federal law enforcement.
- Represented a global retail company in a sophisticated cyberattack involving customized malware targeting payment card data from point-of-sale systems. The crisis response included coordinating the activities of multiple third parties, including state and federal regulators, payment card brand networks, federal law enforcement agencies, and the Department of Justice, as well as directing multiple third-party forensic firms in conducting a technical, forensic investigation.
- Represented a global payments company in an extensive data theft incident by a former employee. The representation included directing a technical forensic investigation, overseeing a complex fraud data analytics analysis, preparing evidence for law enforcement and federal prosecution, and counseling on disclosure and customer communications strategies.
- Represented a global electronics company in connection with a sophisticated reshipping fraud scheme operated out of Eastern Europe impacting high-end electronics and involving multiple vendors.
- Represented one of the world's largest interactive marketing services providers in a massive network breach, involving more than 60 million individual records.
- Worked with a global energy company suspected of being compromised by advanced persistent threat actors. The response included enhanced monitoring of critical systems; preventive forensics, including a breach indicator assessment, a review of existing an investigation, and law enforcement information; and assisting management with briefings to executives.

Cybersecurity Preparedness

- Board Training/Governance and Enterprise Risk Management:
    - Developed training materials for the boards of directors of several companies, including major banks, one of the world's largest construction and industrial equipment rental providers, a global non-car vehicle manufacturer, a global digital media company, and a large insurance company. The presentations and materials highlighted the companies' cybersecurity risks and the legal and regulatory landscape and provided recommendations on overseeing improvements to their companies' data security posture as part of cyber risk management.
    - Presenting annually to the board of directors of one of the largest U.S. financial institutions on issues of cyber risk and cybersecurity, including evaluating the board's duties in this area.

- Breach Response Plan Development:
    - Representing one of the world's largest retailers in developing their worldwide data breach response plan.
    - Developed global breach response plans for a global insurance company with operations in 27 countries.
    - Developed security incident and/or data breach response plans for several global insurance companies, financial institutions, e-commerce companies, retailers, global consulting firms, and digital media corporations.
    - Developed a ransomware-specific breach response for a large telecommunications company.
- Tabletop Exercises:
    - Developed and facilitated cyber tabletop exercises for one of the largest shipment and logistics companies in the world, a global provider of health services, one of the largest financial institutions in the U.S., and several large global insurance companies.
    - Conducted international tabletop exercises in several Asian and South American countries for a global insurance company.
    - Assisted all of these companies with enhancing their breach response strategies and procedures through prioritized recommendations and corrective action plans.
- Cybersecurity Assessments and Legal Reviews:
    - Conducted a cybersecurity preparedness legal review for a large state bank assessing its cybersecurity program against guidance from federal and state financial regulators; presented findings to the board.
    - Conducted an enterprise-wide privacy and data security assessment for a large entertainment media company, assessing its practices for managing and securing sensitive information against a number of laws, regulations, enforcement actions, and guidance materials from regulators. Assisted in performing a risk assessment using the NIST Cybersecurity Framework to enable the company to prioritize its remediation and improvement activities.
    - Advising an independent county agency in a privacy and data security assessment regarding its policies, practices, and procedures. The project includes conducting detailed client interviews, policy review, and preparation of memorandums regarding identified gaps.
    - Performed cybersecurity legal reviews for clients in other industries, such as transportation.
- Representing a financial services information-sharing advisory association on various issues related to information sharing and cybersecurity in the financial services sector.
- Consulting with a number of domestic and international banks on their response to and preparation for recent highly sophisticated and suspected state-sponsored DDoS attacks on their networks.
- Represented a retail industry trade association on issues related to cybersecurity information-sharing mechanisms and related congressional testimony.
- Represented a global telecommunications company in connection with a cloud service provider's security standards accreditation.

- Worked with a global transportation company in developing cybersecurity policies and strategies. The project included ongoing monitoring of federal government initiatives dealing with critical infrastructure cybersecurity and development of appropriate responses, policies, and procedures related to cyber intelligence gathering, information sharing, and cybersecurity practices.
- Worked with an international monetary organization on a multiphased, comprehensive information security risk assessment based on the global information security standard ISO 27001. Our involvement included leading a threat-modeling workshop to help the company understand its current threats and defenses and identify any known gaps in its information security infrastructure, in particular with sophisticated attacks, such as state-sponsored attacks.
- Worked with a multiservices organization on a multiphased, enterprise security risk assessment in which we led an incident response workshop and cyber tabletop exercises to identify any known weaknesses in incident response processes and procedures, in particular with scenarios related to sophisticated cyberattacks and intrusions.
- Worked with a large global consulting firm in an assessment of the company's practices, controls, policies, and procedures concerning the ease with which sensitive client data and company confidential data could leave the company's systems, whether by an inadvertent act by an employee or a malicious act by an insider or outsider.

Privacy-Related Regulatory Inquiries

- Represented a number of clients in federal and state regulatory inquires involving Internet-based practices potentially violating federal and state unfair and deceptive trade practices acts, including a large online advertising company's practices in the use of third-party cookies, a mobile phone carrier's practices in a user's browser experience, and an automotive dealership's practices in collecting user information and monitoring user behavior online.

Publications & Presentations

Publications

- "Policy Shifts May Follow Burst of Defense Cyber Settlements," *Law360*, June 18, 2025.
- "Five Steps for Effective Board Oversight on Cybersecurity Breach Response," *Cybersecurity Law Report*, January 15, 2024.
- "Tips For Balanced Board Oversight After a Cyberincident," *Law360*, April 23, 2024.
- "10 Ransomware Issues GCs Should Have On Their Radar," *Law360*, April 1, 2024.
- "AI Regulation in the U.S.: What's Coming, and What Companies Need to Do in 2023," *Law Journal Newsletters*, February 2023.
- "Mitigating the Risks in Era of Heightened Liability for CISOs," *Bloomberg Law*, November 28, 2022.
- "Uber Exec Trial Is a Lesson in Handling Data Breach Incidents," *Law360*, October 25, 2022.
- "What CFPB, FTC Data Security Crackdown Means For Cos." *Law360*, August 30, 2022.
- "How to Fight Foreign Hackers With Civil Litigation," *Lawfare*, May 13, 2022.
- "FTC Revises the Safeguards Rule and Proposes Mandatory Reporting of Cybersecurity Events," *Westlaw Today,* November 15, 2021.
- "Top 7 Issues All General Counsel Need to Know About Ransomware," *The Computer & Internet Lawyer*, Vol. 38, No. 9, October 2021.
- "How Tech Cos. Can Guard against DOJ Gag Orders," *Law360*, July 22, 2021.

- "Maintaining Attorney-Client Privilege and Work Product Protections over Forensic Reports in Light of '*Wengui v. Clark Hill*,'" *Cybersecurity Law & Strategy,* April 2021.
- "Managing a Cyber Crisis: 7 Practical Tips to Recover with Strength," *Cybersecurity Law & Strategy,* March 4, 2021.
- "The SolarWinds Hack: How Companies Should Assess the Damage," *Bloomberg Law,* January 19, 2021.
- "5 Key Differences In EU And US Breach Notification Regime," *Law360,* December 18, 2020.
- "Vulnerability Management: Increasing Communication to Prevent Problems from Hiding in Plain Sight," *Cybersecurity Law Report,* November 4, 2020.
- "Vulnerability Management: Understanding the Risks of External Scanning," *Cybersecurity Law Report,* October 28, 2020.
- "Vulnerability Management: What You Don't Know from Your External Scans Can Be Used Against You," *Cybersecurity Law Report,* October 14, 2020.
- "A DOJ Demonstration of Shrewd Dark Web Data-Mining," *Law360,* March 26, 2020.
- "Calif. Privacy Law Compliance Strategy for In-House Counsel," *Law360*, December 19, 2019.
- "Carpenter Ruling May Be Turning Point In Digital Data Privacy," *Law360*, August 8, 2018.
- "Working with the Government After a Breach," *CyberInsecurity,* Legal BlackBook, June 2018.
- "New York cybersecurity rules: What firms need to know," *Securities Regulation Daily*, May 24, 2017.
- "Cyber Alert: Breach Roundup, Part II: U.S. and European Data Breach Notification Regulations Highlights and Trends," *Bloomberg Law*, May 1, 2017.
- "NY Governor Cuomo Announces Final NYDFS Cybersecurity Regulations," *Cyberspace Lawyer*, May 2017.
- "Cyber Alert-Breach Roundup, Part 1: State Data Breach Notification Laws Highlights and Trends," *Bloomberg Law*, March 13, 2017.
- "Learning From Experience: Five Actions to Take and Five Mistakes to Avoid When Testing a Breach Response Plan," *The Cybersecurity Law Report,* Vol. 2, No. 20, Oct. 5, 2016.
- "You Don't Need A Data Breach To Face Regulatory Scrutiny," *Law360*, September, 26, 2016.
- "Is Your Company Prepared for a Ransomware Attack?" *Corporate Counsel*, July 11, 2016.
- "3 Ways to Operationalize Cyber-Risk Management," ChiefExecutive.net, October 3, 2015.
- "New Export Requirements on the Horizon for Cybersecurity Products and Technologies," *Intellectual Property & Technology Law Journal*, Vol. 27, No. 9, September 2015.

Presentations

- 26th Annual Institute on Privacy and Cybersecurity Law, Chicago, IL, June 9–10, 2025.
- "Leading Minds of Governance & Tech," National Association of Corporate Directors, Atlanta, GA, April 30, 2025.
- "Incident Response: State of Play," 2025 Incident Response Forum Masterclass, Washington, D.C., April 22, 2025.
- "Countering Sophisticated Threats: Insights from the Frontlines,", Denver, CO, September 18–19, 2024.
- 25th Annual Institute on Privacy and Cybersecurity Law, Practising Law Institute, Chicago, IL, June 3–4, 2024.

- "Cyber War Stories from the Frontlines: From Ransomware to Hacking Back" ABA Privacy and Emerging Technology Institute and Spring Meeting, American Bar Association, Rockville, MD, April 17–19, 2024.
- "State of Play: LockBit, Scattered Spider, and Other New Ransomware Variants," Incident Response Forum Ransomware 2024, webinar, January 18, 2024.
- "Managing a Cybersecurity Incident," Corporate Counsel Institute 2023, State Bar of Georgia, Atlanta, GA, December 14–15, 2023.
- Twenty-Fourth Annual Institute on Privacy and Cybersecurity Law, Chicago, IL, June 5-6, 2023.
- "Ransomware Attacks: What to Do When You Get the Call," Incident Response Forum Ransomware 2023, January 12, 2023.
- "Uber Verdict: The CISO, The Law, and The Door!" Aqua Security, webinar, December 5, 2022.
- "A Wolf in Sheep's Clothing? How Data Protection Laws Regulate AI" ABA Science & Technology Law Section's AI & Robotics 2022, October 10-11, 2022.
- "Keeping Up with the Latest Cybersecurity Challenges," PLI's 23rd Annual Institute on Privacy and Cybersecurity Law, Chicago, IL, June 6-7, 2022.
- "Are You Sure You're Doing That Right? A Mock Hearing," RSA Conference 2022, San Francisco, CA, February 6-10, 2022.
- "Ransomware – Lessons Learned from the Trenches," Georgia Bar Corporate Counsel, webinar, December 7-10, 2021.
- "Combating and Outpacing Ransomware: Yes, it's Possible," Uniting Women In Cyber Conference 2021, webinar, October 4-6, 2021.
- "That's Secret—Can a Forensic Report be Protected as a Privileged Work Product?" 2021 National Cyber Summit, Huntsville, AL, September 26-30, 2021.
- "Private Sector Cybersecurity: The Changing Landscape," American Bar Association's Standing Committee on Law and National Security and Cybersecurity Legal Task Force, webinar, August 3, 2021.
- "It's Been a Privilege to Serve You–A Mock Hearing," RSA Conference 2021, webinar, May 17-20, 2021.
- "The Public & Private Sector's Role in Cybersecurity," Cardozo's Women in Tech Law (WiTL), webinar, April 19, 2021.
- "Incident Response: Attorney-Client Privilege and Work-Product Protection," Incident Response Forum Masterclass 2021, webinar, April 8, 2021.
- "Meeting the Moment," Ms. JD's 12th Annual Conference on Women in the Law, webinar, March 11, 2021.
- "Asset Discovery and Visibility," Cybersecurity Leadership Series Panel, webinar, January 25, 2021.
- "Ransomware and Healthcare Organizations," Incident Response Forum Ransomware 2021, webinar, January 14, 2021.
- "Virtual Roundtable," The Cybersecurity Law Report, webinar, January 13, 2021.

Professional & Community Engagement

- U.S. Secret Service, Cyber Investigation Advisory Board (2022-present)
- Certified Information Systems Security Professional (CISSP)
- National Association of Corporate Directors CERT Certificate in Cybersecurity Oversight

- American Bar Association, Section of Science and Technology Law and Litigation Section
- American Friends of the Alexander von Humbolt Bundeskanzler Foundation, board of directors
- CyberTheory, CISO advisory board
- Sedona Conference on Cyber Liability, faculty (2013–present)
- Georgetown University Law Center Cybersecurity Law Institute, co-chair (2015–present)
- PLI Twenty-Third Annual Institute on Privacy and Cybersecurity Law, co-chair (2022, Chicago)
- Georgetown University Law Center Cybersecurity Law Institute, advisory board (2013–2015)
- Financial Services Information Sharing and Advisory Center, board adviser (2010–2012)
- eFraud Network, Program Committee (2008–2011); e-Privacy Committee, co-chair (2012–present); councilmember and budget officer (2004–2009)
- ABA Section of Science and Technology Law, Information Security Committee, co-chair (2001–2004)
- Alexander von Humbolt Bundeskanzler Foundation, Bonn, Munich, Germany, 1996–1997
- Fellow: Liaison with German government officials and business leaders

Court Admissions

- United States Court of Appeals for the Ninth Circuit
- United States Court of Appeals for the District of Columbia Circuit
- United States District Court for the District of Columbia

Accolades

- *Chambers USA* – Privacy and Data Security: Cybersecurity (2017 – Present)
- *Chambers Global* – Privacy & Data Security: Cybersecurity (2018 – Present)
- *The Best Lawyers in America*® – Privacy and Data Security Law (2023 – 2025)
- *Legal 500* – Cyber Law "Leading Lawyer" (2022 – present)
- Cybersecurity Docket "Incident Response 40" (2016 – present)
- *SC Magazine* – "Industry Pioneer"
- BTI Consulting Group – "Client Service All-Star"
- *Washingtonian* – "Top Lawyers – Cybersecurity"
- Burton Award for Legal Achievement – "Cybersecurity: What Directors Need to Know in an Era of Increased Scrutiny"

Education

- University of Munich, Germany (LL.M., 1997)
- Georgetown University (J.D., 1996)
- University of Wisconsin (B.A., 1992)

Languages

- German

Admitted to Practice

- District of Columbia
- Illinois
- U.S. Supreme Court