Privacy and Cybersecurity
Compliance, Preparedness and Rapid Response

Skadden

Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates

The Americas
Boston
Chicago
Houston
Los Angeles
New York
Palo Alto
São Paulo
Toronto
Washington, D.C.
Wilmington

Europe
Brussels
Frankfurt
London
Moscow
Munich
Paris

Asia Pacific
Beijing
Hong Kong
Seoul
Shanghai
Singapore
Tokyo

Cybersecurity is a top priority for every organization. Given the potentially catastrophic consequences of cyberattacks, together with the regulatory scrutiny, enforcement activity and private class action litigation likely to follow, cybersecurity has become a cost of staying in business.

40%

more data breaches reported in 2016 compared to 2015.

– ITRC Data Breach Report 2016

$4M

average cost for organizations per data breach, a 29 percent increase since 2013.

– Ponemon 2016 Cost of Data Breach Report

Cyberattack preparedness, coupled with a well-developed and tested Security Incident Response Plan (SIRP), is essential for mitigating the legal, operational and reputational risk arising from cyber threats. Engagement with outside counsel who know the legal and regulatory landscape and the key areas of potential liability exposure is a critical part of any company's cybersecurity strategy. The breadth of our skills, the depth of our expertise and the extent of our experience has earned the confidence of our clients to call on us both before and during a cyberattack.

Privacy
Advisory Services and Compliance

Companies are gathering and storing increasing amounts of information about their customers, and finding innovative ways to monetize that information. This has been fueled, in part, by an increase in innovative mining and analytic tools that are available to companies. However, these monetization opportunities have drawn the close attention of regulators, government officials and plaintiffs' lawyers. Companies that do not have robust privacy programs are facing increased legal exposure, including the possibility of long-term regulatory consent decrees.

For over 20 years, Skadden has added value to clients by assisting them in navigating the rapidly changing privacy and technology landscapes to mitigate their legal risk, and help them maximize their revenue opportunities.

GLOBAL PRIVACY POLICIES

Many of our clients use and distribute data across multiple geographic regions and across multiple device types. We counsel clients on establishing and maintaining global privacy policies that are customized to the requirements of individual countries. As part of these engagements, we meet with clients to discuss their current and future use of personal data to establish an overall strategy. We take this information and develop a global privacy approach. Once these privacy structures are in place, we work with clients on an ongoing basis to update them as laws and regulations, or the company's own business needs, evolve.

Our group also works with clients to understand and comply with cross-border data flow requirements in a manner that is best suited for their business needs. With respect to data transfer out of the EU, we advise clients on model contracts and binding corporate rules, and also assist clients with certifying to the EU-U.S. Privacy Shield.

EU GENERAL DATA PROTECTION REGULATION

The upcoming EU General Data Protection Regulation (GDPR) will impose a variety of new requirements on companies accessing the data of EU residents. Skadden works closely with clients to help them understand the scope and applicability of the GDPR and to design compliance programs so that they are prepared to meet the GDPR requirements when they go into effect in 2018.

PRIVACY AUDITS AND COMPLIANCE PROGRAMS

Regulators and plaintiffs' lawyers increasingly are focusing on how companies collect and use personal information. Their focus not only is on compliance with privacy laws, but also on whether the company is using personal information in a manner that is consistent with their privacy policies and marketing materials. When regulators, such as the Federal Trade Commission (FTC), have brought enforcement actions they are not merely pursuing "bad actors." Rather, they also are bringing enforcement actions against companies that may have inadvertently acted contrary to what they represented to their consumer. A privacy audit helps companies eliminate these potential areas of liability, and engenders a culture of vigilance with respect to privacy compliance that extends beyond the audit itself.

As part of our privacy audits we:

- Ensure the client collects and utilizes personally identifiable information (PII) in a manner that complies with applicable legal requirements as well as statements it has made to customers and employees;
- Ensure the company is in compliance with any data use restrictions imposed by third parties, including social media platforms;
- Establish internal processes and create policies to ensure that PII always is used in a manner that complies with applicable legal requirements and external and internal disclosures;
- Establish a data map of how information is collected, used, managed, stored and distributed internally and externally that can be updated and monitored on a regular basis;
- Establish a process for ensuring local law compliance and, outside the U.S., for interacting with applicable data protection authorities;
- Establish ongoing training and monitoring programs; and
- Review and/or create all necessary policies and procedures.

REGULATORY COMPLIANCE

We advise clients on the steps necessary to comply with all privacy regulations, including the Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, the Fair and Accurate Credit Transactions Act, the Children's Online Privacy Protection Act (COPPA), the CAN-SPAM Act, and the Telemarketing Sales Rule and the Telephone Consumer Protection Act. We counsel clients on how industry trends and new protocols may impact the use of personal information, and help them find innovative solutions that allow them to utilize the information they have without violating any legal requirements. Our attorneys also closely track developments at the state and federal levels to ensure that our clients always are fully informed about, and fully compliant with, any changes in the legal and regulatory environment.

POLICIES AND PROCEDURES

Skadden works with clients to create and review a wide range of privacy compliance documents, including:

- External facing privacy policies;
- Internal employee policies guiding the use of PII;
- Statements to be used in marketing collateral regarding privacy policies;
- Written Information Security Programs (WISPs);
- Cross-border data flow documentation; and
- Language regarding privacy to include in vendor agreements.

DATA MONETIZATION

Our clients are increasingly looking for ways to monetize the data they hold, including through new "big data" analytics tools. We negotiate third-party vendor agreements in this space, and advise clients on whether their planned programs comply with their privacy policies and applicable laws.

PRIVACY BY DESIGN

Regulators expect companies to engage in "privacy by design" — the concept that privacy consideration should be an integral part of the development process for any product or service. We work with clients to develop "privacy by design" programs that minimize the legal risk that PII is used in a manner that might draw regulatory scrutiny or invite a lawsuit. Companies that engage in privacy by design programs find that they save money by avoiding the need to "back-fill" privacy protections after a new product or service has been finalized.

THE INTERNET OF THINGS

Regulators, such as the FTC, are increasingly focused on the "internet of things" and its privacy implications. We work with clients on understanding the regulatory environment and on designing products that take this environment into account.

Cybersecurity Preparedness Services

Companies today appreciate the importance of implementing the most up-to-date information security technology to prevent or minimize the impact of a cyberattack. But a company's cyber-preparedness cannot end there. The key issues in enforcement actions and litigation following a cyberattack are how the company managed its cybersecurity planning before the attack, and how it responded during an attack. Companies should expect questions about their cybersecurity governance structure, the level of engagement by C-suite executives and board members, and the quality of the company's crisis response plan. In building their case, the government and private plaintiffs also will scour the company's internal and public statements about cybersecurity risk, looking for potentially damaging statements.

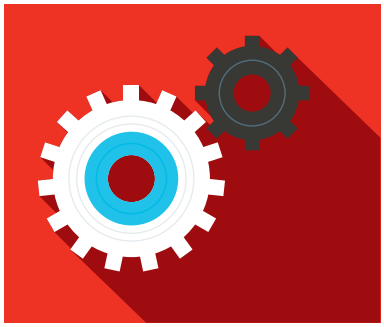
To best manage a cyber-incident, companies today need to build a "legal firewall." Skadden's Privacy and Cybersecurity Group has the experience to help companies uncover and address their legal vulnerabilities in an efficient and cost-effective manner.

DEVELOPMENT AND REVIEW OF SECURITY INCIDENT RESPONSE PLANS (SIRP)

One of the most important steps a company can take before a cyberattack is to develop and test a SIRP. Studies have shown that companies that have a tested SIRP in place respond more efficiently and effectively to an attack — a key factor in risk mitigation. We help clients create SIRPs, or review existing ones to ensure they reflect best practices and address the legal issues most likely to arise around an incident. Because the quality of the SIRP and how it was executed will be a likely focal point of regulatory actions and litigation, building the SIRP from a legal perspective is essential. We also routinely work with clients to "table test" their existing plans, pointing out legal and practical issues that may arise during an attack.

CYBERSECURITY "AUDITS"

In any regulatory enforcement action or litigation, the regulator or private plaintiff will rely on the documentary record to establish the company's negligence in managing cybersecurity or usage of personal information. We review clients' documentation relating to cybersecurity and privacy to help determine whether (i) the company has made statements that are inconsistent with, or overstate, the company's cybersecurity planning; (ii) external consultants highlighted proposals or concerns that were not adequately addressed; and (iii) employees are properly notified of their obligations when handling data and sensitive information. We conduct this review through a "litigation lens," always thinking of what issues may come up in litigation and how to mitigate those concerns as part of a company's preparedness program. As part of this exercise, we also review whether a client's use of personal information, including internal and external data flows, is consistent with its stated policies and regulatory obligations.



"The persistently high levels of hacking and malware attacks of all kinds are a reminder that organizations across industries, and of all sizes, need actionable plans ready to implement when a breach occurs."

– Beazley Breach Insights 2016

DEVELOPMENT AND REVIEW OF CYBERSECURITY GOVERNANCE MODELS

Regulators and private plaintiffs carefully scrutinize a company's cybersecurity governance. They ask whether information security officers had clear accountability and access to senior management and the board, and whether the board was sufficiently informed. We help clients develop appropriately tailored cybersecurity governance practices and review the governance that clients already have in place. We advise on whether changes may be warranted to bring a client's governance in line with regulatory expectations and best practices.

RISK ASSESSMENT ANALYSIS

Risk assessment is a fundamental building block, as well as a best practice, of cybersecurity planning. We work with clients to help identify and assess these risks, drawing on our wide range of expertise conducting such assessments from a legal perspective. This includes determining the company's most valuable assets, how they are protected and who can access that information. Where clients have already conducted such an assessment, we review and comment on their assessment to determine if it meets accepted practices.

POLICIES AND PROCEDURES

The Skadden Privacy and Cybersecurity Group has experience creating and reviewing all of the policies and procedures companies require, including external-facing security policies, internal policies guiding the use of PII and cybersecurity, statements to be used in marketing collateral regarding security policies, written information security policies (WISPs) and language regarding cybersecurity to include in third-party contracts.

EMPLOYEE TRAINING

A company's cybersecurity planning is only effective if employees are sensitized to the related risks through training. While companies generally design and implement such training internally, we work with clients develop the scope and level of training that should satisfy a regulatory inquiry and best protect the company if its practices were challenged in a litigation.

INSURANCE

Cyber insurance is a critical aspect of mitigating cybersecurity risk. Our insurance team works with clients to review existing policies to determine whether cyber insurance is warranted, help clients negotiate cyber insurance coverage and advise on the scope of coverage if an attack occurs.

VENDOR MANAGEMENT ASSESSMENT

One of the most critical threat vectors that companies face is cyberattacks that exploit a third-party vendor's network connection to a company. We review clients' vendor management processes to determine if appropriate cybersecurity requirements are in place and review third-party vendor agreements to determine if the client is adequately protected.

Cybersecurity Rapid Response Services

When a company discovers it is the victim of a cyberattack, every moment is critical. Companies not only must contain the attack and mitigate the damage, they also must quickly manage an array of demands and pressures from the media, government officials, customers, business partners and shareholders. Companies also must be prepared for the reality that bloggers and the media can sometimes break the news of an attack before a company is able to gather all the relevant facts, and that regulators and government officials are demanding faster response times and want to be informed immediately. The rapidity and efficiency with which a company responds to a cyberattack is now a subject matter of regulatory inquiry and claims asserted by private plaintiffs. Skadden's multidisciplinary Cyberattack Rapid Response Team has the knowledge and experience to help companies manage an attack and minimize legal exposure.

FORENSICS

The Skadden team includes attorneys with technology and cybersecurity experience who can work with a client's forensic experts to evaluate the cyberattack, and determine the best way to approach remediation efforts. Skadden has strong working relationships with the leading forensics providers and can help clients select the appropriate teams given their specific needs.

LAW ENFORCEMENT AND REGULATORS

The Skadden team includes former government officials who can advise clients on the roles of various agencies, including regulators and law enforcement, and appropriate ways to work with them. Skadden has extensive experience with numerous agencies, including the FBI Cyber Division, the Computer Crime and Intellectual Property Section of the Department of Justice, the Secret Service, the Department of the Treasury, the Department of Homeland Security and various independent regulatory agencies.

DATA BREACH NOTIFICATION

The Skadden team stays up to date on all current state and federal data breach notification requirements. We can rapidly advise clients on whether disclosure to affected individuals is required and manage multistate notification processes.

PUBLIC DISCLOSURES

Skadden has a long history of helping clients make appropriate public statements during a crisis. In the case of a cyberattack, it is important to review all public statements to ensure that they are consistent with legal requirements. We have close working relationships with communications and public relations firms with experience in cyberattack response.

SEC AND REGULATORY DISCLOSURES

The Skadden team includes attorneys with SEC and regulatory experience who quickly help clients assess whether disclosure is required under SEC filings or as a result of the company's regulatory obligations, and draft any necessary disclosures. We also work with clients on any presentations or reports they need to make to regulators.

C-SUITE AND BOARD SUPPORT

Cyberattacks can quickly become C-Suite and board-level issues. Skadden team members routinely advise boards on critical company matters, and we have the experience to advise senior management and boards on cyberattacks, the company's risk exposure and the path forward.

LITIGATION

Class action and shareholder derivative lawsuits are a reality following any cyberattack. The Skadden team includes members of our Mass Torts, Insurance and Consumer Litigation Group, who can prepare the company for any type of class action lawsuits and defend against ensuing litigation.

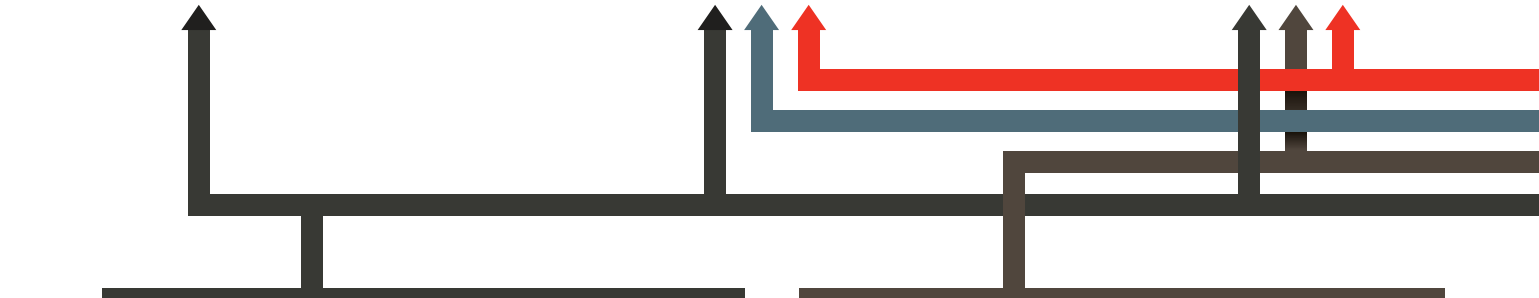
How Skadden Can Partner With You

Skadden's broad and diverse practice areas provide a unique platform from which we can assist clients at every stage of the cybersecurity life cycle. Our coordinated, multidisciplinary team can mobilize for a client at a moment's notice. Our integrated CRRT provides strategic counsel on substantive issues of privacy and cybersecurity; addresses corporate governance and director responsibility concerns; navigates any concurrent civil, criminal and/or administrative proceedings; and helps manage cyber insurance claims.

Privacy and Cybersecurity Assessment

Compliance Obligations

Risk Management



Privacy and Cybersecurity

Key Contacts:
Stuart Levi
James Talbot
Jessica Cohen

Our attorneys help companies navigate and comply with the evolving privacy and cybersecurity landscape in order to maximize the ROI of data usage while avoiding legal risk. We are well-versed in privacy laws and regulations worldwide and understand the business models and technologies underlying data usage. Our group advises companies on how to adopt "privacy by design" techniques, draft and implement privacy and security policies, create "rapid response teams," and establish internal governance and reporting systems to minimize liability exposure in the event of a cybersecurity incident.

Corporate Goverance

Key Contacts:
Marc Gerber
Stuart Levi
Patrick Fitzgerald
Michael Scudder

The firm has a long history of successfully representing our clients in critical incident situations. In particular, we are highly attuned to the disclosure and regulatory requirements that arise in the context of a privacy or cybersecurity incident, and together with our clients, we develop and execute strategies for responding to governmental agencies, shareholders, the investment community and the media.

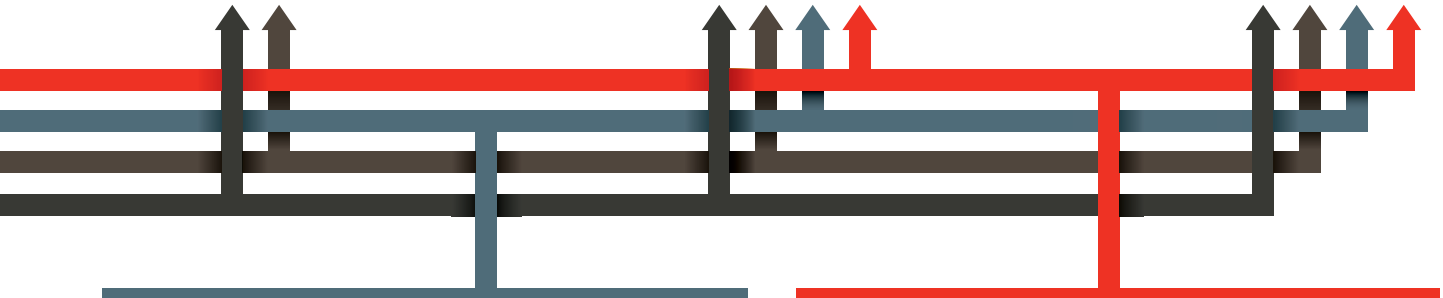
What distinguishes Skadden is that they provide a high level of service and are excellent in every single area that they offer support on. They are remarkable.

– 2016 *Acritas* U.S. Law Firm Brand Index

Critical Incident Management

Mass Litigation

Law Enforcement Cooperation



Mass Torts, Insurance and Consumer Litigation

Key Contacts:
John Beisner
Jessica Miller

We have represented numerous clients, including a wide variety of *Fortune* 500 companies, in many of the significant mass litigations of the last 20 years. The firm stands out for its depth, breadth and innovative strategies in defending class action lawsuits and is uniquely equipped to counsel clients in class actions brought by consumers whose data was compromised. We also assist clients in navigating their cyber insurance policies.

Government Enforcement and White Collar Crime

Key Contacts:
Patrick Fitzgerald
Michael Scudder
Stuart Levi

Skadden's powerful combination of resources across the U.S. and internationally is ideally suited to helping companies decide how to interact with law enforcement and other government agencies in a cybersecurity incident, including how best to utilize government resources to protect the organization. Skadden attorneys have close working relationships with a number of key members of the government's cybersecurity community and can provide unmatched strategic advice to clients.

Relevant Experience

CYBERSECURITY ATTACKS

We have worked with numerous clients to help them manage cyber-security attacks and their aftermath, including data breaches, theft of confidential information, denial of service attacks and "ransomware" attacks. Our clients include companies in the media, financial services, manufacturing, insurance, online service and retail industries.

DATA BREACH NOTIFICATIONS

We have represented numerous companies across multiple industry sectors in drafting and disseminating multistate data breach notifications that were required under law and in advising when notification was not required.

INTERACTION WITH GOVERNMENT

We have coordinated interaction with federal and state criminal and civil enforcement authorities in connection with their investigations of multiple clients regarding cybersecurity intrusions and/or alleged criminal conduct on the part of employees.

PRIVACY AND CYBERSECURITY AUDITS

We have reviewed the privacy and cybersecurity programs and statements of multiple companies across a wide range of industries to identify and remediate any issues that may expose the client to risk.

GLOBAL PRIVACY AND CYBSERCURITY PROGRAMS

We have represented numerous global companies across multiple industry sectors in drafting external-facing and internal employee privacy policies. As part of this process, we have helped companies create implementation and training programs and conducted audits to monitor compliance.

TRANSBORDER DATA FLOW

We have advised numerous companies on the optimal approach to move data around the world. This has included drafting model contracts, assisting companies with Safe Harbor certification and structuring data flows to comply with local regulatory requirements.

SPECIFIC LITIGATION AND REGULATORY REPRESENTATIONS:

Chase Manhattan Bank against allegations that Chase violated its own consumer privacy and confidentiality policies by sharing personally identifiable information about its credit card and mortgage customers with third-party vendors. The New York Appellate Division, Second Department affirmed the New York Supreme Court's dismissal of this case.

Citigroup in a privacy class action alleging invasion of privacy torts and Section 17200 violations by sharing customer information with third-party vendors.

A commercial bank in a:

– privacy class action alleging statutory and common law invasion of privacy torts, contract claims and state statutory claims related to third-party intrusion to obtain credit and debit card information and other personal identifying information contained on a retailer's computer system; and

– nationwide putative class action alleging negligence, breach of contract, negligent misrepresentation and statutory claims related to third-party intrusion of a retailer's computer system to obtain credit and debit card information and other personal identifying information.

Farmers Insurance Exchange in securing a favorable settlement of computer trespass claims that Farmers brought against the Auto Club Group in the U.S. District Court for the Northern District of Illinois charging that Auto Club violated the federal Computer Fraud and Abuse Act and state computer trespass statutes after Farmers discovered that Auto Club employees illegally accessed its proprietary computer databases.

A national mortgage company in a privacy class action alleging invasion of privacy torts and unfair and deceptive trade practices violations by information sharing and telemarketing with respect to mortgage customers.

Hummingbird USA Inc. in contract and tort claims arising from the loss of computer equipment on which private information of 1.8 million customers of a state student loan agency was stored and in connection with the response to Texas Public Information Act requests regarding the same incident.

An Internet services company in connection with an investigation by the New York state attorney general and FTC into its online privacy practices.

A medical records company in connection with civil and criminal issues related to a hack into personal medical records.

NIC, Inc., operator of the RI.gov website on behalf of the state of Rhode Island, in connection with the theft of Social Security numbers, driver's license numbers, and credit and debit card numbers.

The Securities Industry and Financial Markets Association as plaintiff in obtaining a preliminary injunction in its lawsuit seeking to protect the constitutional rights of its member banks' senior employees and their families by preventing the state of Connecticut from enforcing a provision of the Connecticut Campaign Finance Reform Act that required the collection, disclosure and publication on the Internet of the identities of spouses and dependent children of certain officers and employees of state contractors and prospective state contractors.

A website security provider in a lawsuit in connection with a hack into the website of a state government resulting in stolen credit card information from individuals who had done business online with state agencies.

Cybersecurity Rapid Response Team

Stuart D. Levi
New York / Intellectual Property and Technology, Privacy and Cybersecurity

Stuart Levi is co-head of Skadden's Intellectual Property and Technology Group, and coordinates the firm's privacy and cybersecurity practice. In the area of privacy and cybersecurity, Mr. Levi advises clients on complying with data privacy laws, drafts external and internal privacy policies, represents clients in FTC privacy investigations, helps clients prepare for cybersecurity incidents, and assists clients in implementing effective responses to cybersecurity attacks, including data breach notifications, working with law enforcement and providing crisis management counseling. Mr. Levi also has a broad and diverse practice in the areas of intellectual property and technology transactions, including licensing, strategic acquisitions and joint ventures.

Marc S. Gerber
Washington, D.C. / Corporate Governance

Marc Gerber concentrates his practice in the areas of mergers and acquisitions, corporate governance, and general corporate and securities matters. Mr. Gerber represents numerous clients on a full range of corporate governance and related matters, including advising on the rules and regulations of the SEC. Mr. Gerber counsels companies, boards of directors and board committees on corporate governance topics such as shareholder rights plans, advance notice bylaws, proxy access, board independence, board self-evaluation and cybersecurity.

Patrick J. Fitzgerald
Chicago / Government Enforcement and White Collar Crime

Patrick Fitzgerald is a seasoned trial lawyer and experienced investigator whose practice focuses on internal investigations, government enforcement matters and civil litigation. Prior to joining Skadden in 2012, Mr. Fitzgerald most recently served as the U.S. attorney for the Northern District of Illinois. Appointed in 2001 by President George W. Bush, he was the longest-serving U.S. Attorney ever in Chicago. During his tenure at the U.S. attorney's office, he was involved in numerous significant national security investigations and contributed to a number of nationwide initiatives, including having served on the Illinios attorney general's Critical Incident Response Group.

John H. Beisner
Washington, D.C. / Mass Torts, Insurance and Consumer Litigation

John Beisner is the leader of Skadden's Mass Torts, Insurance and Consumer Litigation Group. He focuses on the defense of purported class actions, mass tort matters and other complex civil litigation in both federal and state courts. Over the past 25 years, he has defended major U.S. and international corporations in more than 600 purported class actions filed in federal courts and 40 state courts, at both the trial and appellate levels. He also has handled numerous matters before the Judicial Panel on MDL litigation, as well as proceedings before various federal and state administrative agencies. In addition, Mr. Beisner was instrumental in the passage of the Class Action Fairness Act of 2005 (CAFA).

Cybersecurity Rapid Response Team

Michael Y. Scudder, Jr.
Chicago / Government Enforcement and White Collar Crime

Michael Scudder concentrates in commercial litigation, white collar crime, government investigations and accounting issues. Before joining the firm in 2009, Mr. Scudder was a White House legal adviser under President George W. Bush from 2007-2009. In this capacity, he served as general counsel of the National Security Council and advised the president and senior administration officials on defense, intelligence, legislative and litigation matters. Prior to that senior role, he provided legal advice on national security matters at the Department of Justice. As a result of his involvement providing security advice at the highest level of government, Mr. Scudder continues to maintain a very high security clearance.

Jessica D. Miller
Washington, D.C. / Mass Torts, Insurance and Consumer Litigation

Jessica Miller has broad experience in the defense of purported class actions and other complex civil litigation with a focus on product liability matters and MDL litigation proceedings. Ms. Miller has been responsible for case coordination, strategy, and law and motions in numerous federal and state court coordinated proceedings involving pharmaceutical products, medical devices and industrial products. Together with John Beisner, Ms. Miller was instrumental in the passage of CAFA.

Joshua F. Gruenspecht
Washington, D.C. / Communications

Joshua Gruenspecht advises clients and drafts agreements and filings in a variety of transactional, regulatory and litigation matters, including cross-border transactions, negotiated service agreements, regulatory filings and advocacy, and privacy and cybersecurity issues. Mr. Gruenspecht practices in the media, telecommunications, technology and defense sectors, among others. Prior to law school, Mr. Gruenspecht worked as an engineer specializing in communications technologies and computer network exploitation for the federal government and BBN Technologies.

James S. Talbot
New York / Intellectual Property and Technology

James Talbot's practice focuses on the intellectual property aspects of transactional matters. His practice also includes Internet domain name matters, and he has worked with clients on issues relating to top-level domains, domain name registration and monitoring, and domain name disputes. Since joining the firm in 1997, Mr. Talbot has counseled a broad array of clients, both large and small, covering a wide range of businesses. He has advised on and negotiated agreements relating to outsourcing arrangements, asset and stock purchases, and developing and licensing technology and intellectual property.

Cybersecurity Rapid Response Team

Jessica N. Cohen
New York / Intellectual Property and Technology, Privacy and Cybersecurity

Jessica Cohen focuses on intellectual property and technology issues in a wide variety of transactions, including licensing and development agreements, outsourcing agreements, service agreements, strategic alliances, and mergers and acquisitions. Ms. Cohen counsels clients both large and small on intellectual property protection and ownership issues, and technology implementation and maintenance issues.

Peter Luneau
New York / Mass Torts, Insurance and Consumer Litigation

Peter Luneau represents clients in a variety of complex insurance coverage and product liability matters. His representation of clients covers a wide range of insurance coverage disputes, including, for example, multiparty litigation in state and federal courts concerning business interruption, environmental and property losses, and numerous U.S. and international insurance and reinsurance arbitrations and alternative dispute resolutions.