PROGRAM AGENDA

April 23, 2013

Time	Session	Speakers
8:30 – 8:50 am	**Registration and Breakfast**	
8:50 – 9:00 am	**Welcome and Introductions**	*Paul Theiss; Philip Recht*
9:00 – 9:45 am	**Cyber Security Threats – What They Mean for Homeland Security and Economic Growth**	*Richard Ben-Veniste; Richard Clarke*
9:45 – 10:45 am	**The Effect on Business of the Executive Order, Proposed Legislation, and SEC Guidance**	*Jake Olcott; Jeff Taft; Howard Waltzman; Richard Rosenfeld*
10:45 – 11:00 am	**Break**	
11:00 – 12:00 pm	**Cyber Vulnerabilities – Identifying Legal Risk and Approaches for Risk Mitigation**	*Rebecca Eisner; Archis Parasharami; Jonathan Cooperman; Larry Collins*
12:00 – 1:00 pm	**Networking Luncheon**	

MAYER·BROWN

GOOD HARBOR
SECURITY RISK MANAGEMENT, LLC

Acknowledging and Preparing For the Growing Threat of Cyber Attacks

Richard Ben-Veniste
Partner, Mayer Brown
+1 202 263 3333
rben-veniste@mayerbrown.com

Richard A. Clarke
Chairman & CEO, Good Harbor Security Risk Management, LLC
+1 703 945 1307
rclarke@goodharbor.net

Quantifying the Growing Threat

- Worldwide, 2012 saw 2,644 reported incidents of data breach, more than double the previous year. The business sector accounted for more than 60% of these incidents.
- In 2012, it took companies an average of 24 days to resolve an attack, with a cost of over $24,000 per day.
- Total economic loss from a data breach (can include revenue loss, business disruption, equipment damages, legal costs, etc.) can reach into the millions.
- Average data breach class-action settlement award is $2,500 per plaintiff, with plaintiffs' attorneys' fees averaging around $1.2 million.

Multitude of Threats & Motives

- External hacking to steal customer information and trade secrets.
- Malware and denial of service attacks aimed at disrupting business.
- Extortion by organized crime groups and others.
- Protests by activists.
- Internal sabotage by disgruntled employees.
- Negligence: lost devices, unintended release of information, including social security numbers, passwords, birthdates, medical information, etc.

Cautionary Tales

Nationwide Insurance

- Data breach in October 2012 exposed records of 1.1 million customers.
- Overseas hackers responsible.
- Information included names, birth dates, social security numbers, and driver's license numbers.

Saudi Aramco

- Cyber attack on world's largest oil company in August 2012.
- 30,000 computers damaged.
- Internal network shut down for more than a week

Cautionary Tales, cont'd.

Global Payments Inc.

- In March 2012, hackers accessed payment databases of the credit card processor. 7 million accounts exposed.
- Breach cost the company $94 million in 2012.
- Company expects to spend another $35 million in 2013.

Zappos.com

- Hackers accessed customer database of online shoe retailer in January 2012.
- Accessed records of approximately 24 million customers.
- Company is now facing dozens of class action lawsuits.

Government Response – Prevention, Disclosure, & Punishment

- President issues executive order in February to facilitate private-public information sharing.
- Pending Cyber Intelligence Sharing and Protection Act (CISPA) has the same goal – more comprehensive and controversial.
- 46 states have laws requiring businesses to disclose data breaches involving personal information.
- FTC and HHS have begun imposing fines and instituting enforcement actions over breaches involving customer and patient personal information.
- SEC guidance mandates disclosure of risk and incidents.

You Don't Need a Weatherman ...

- Lessons learned from 9/11
- Catastrophic attack could bring down entire sectors of the economy, shake consumer confidence for years to come.
- Result could be inefficient and onerous data security and reporting requirements.
- What is voluntary now, will become mandatory.

How Mayer Brown Can Help

- Assist clients in preventing and responding to data breaches and developing notification policies.
- Advise clients on new regulations and help develop compliance policies.
- Assess U.S. and international clients' security and privacy procedures and policies.
- Provide world-class representation in litigation and government compliance investigations.

Cyber Threat

Into the Breach
MANAGING CYBER SECURITY THREATS IN THE DIGITAL AGE

"America's economic prosperity in the 21st century will depend on cybersecurity"

President Barack Obama

"We know that foreign cyber actors are probing America's critical infrastructure networks. They are targeting the computer control systems that operate chemical, electricity, and water plants."

Leon Panetta

Former Secretary of Defense

"The loss of industrial information and intellectual property though cyber espionage constitutes the greatest transfer of wealth in human history."

Gen. Keith Alexander

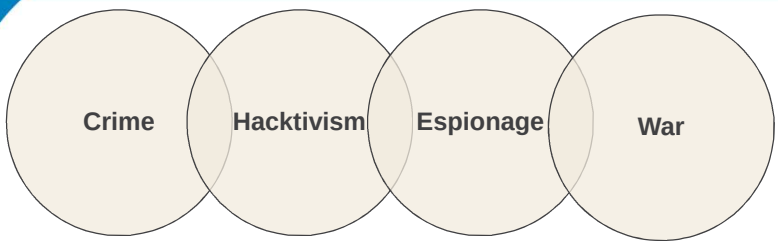
Director, National Security Agency

GOOD HARBOR SECURITY RISK MANAGEMENT, LLC

MAYER·BROWN

Four Forms of Cyber Attacks

Into the Breach
MANAGING CYBER SECURITY THREATS IN THE DIGITAL AGE



Crime

Unauthorized computer penetration for immediate financial gain through fraud or blackmail

Espionage

Unauthorized computer penetration to acquire sensitive or valuable information to gain competitive advantage

Hacktivism

Use of cyber attacks as a form of politically or ideologically motivated protest

War

Use of cyber attacks to cause damage through severe disruption or damage of computer controlled systems

GOOD HARBOR SECURITY RISK MANAGEMENT, LLC

MAYER·BROWN

Business Secrets Are at Risk

Into the Breach
MANAGING CYBER SECURITY THREATS IN THE DIGITAL AGE

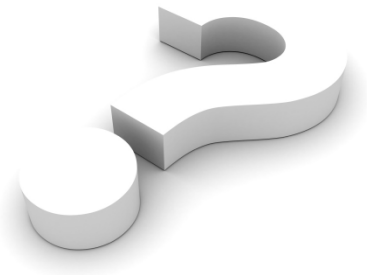
What types of data reside on your IT networks?

- New product designs? Blueprints? Formulas?
- Pending copyright patent and data?
- Financial information?
- Customer-sensitive data?
- Research and Development information?
- Upcoming competitive bid information?
- Information with reputational implications?
- Proprietary operational information?

GOOD HARBOR SECURITY RISK MANAGEMENT, LLC

MAYER·BROWN

QUESTIONS?



MAYER·BROWN

GOOD HARBOR
SECURITY RISK MANAGEMENT, LLC

The Effect on Business of the Executive Order, Proposed Legislation, and SEC Guidance

Jake Olcott
Principal, Good Harbor
+1 703 945 1307
jacob.olcott@goodharbor.net

Richard Rosenfeld
Partner, Mayer Brown
+1 212 506 2178
rrosenfeld@mayerbrown.com

Jeff Taft
Partner, Mayer Brown
+1 202 263 3293
jtaft@mayerbrown.com

Howard Waltzman
Partner, Mayer Brown
+1 202 263 3848
hwaltzman@mayerbrown.com

Cyber Security Executive Order

- On February 12, 2013, President Obama issued an executive order intended to improve the cyber security of "critical infrastructure" in the United States.
- The Order seeks to build a public-private partnership with the owners and operators of critical infrastructure, to improve information sharing, and to collaboratively establish risk-based cyber security standards.

Critical Infrastructure

- The definition of "critical infrastructure" is broad and includes "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

Information Sharing

- The Order promotes information sharing by expanding the Enhanced Cybersecurity Services program and providing both classified reports on cyber threats to authorized entities and unclassified reports to other entities.
- However, the Order provides neither an exemption from certain privacy laws—such as the Electronic Communications Privacy Act—that serve as an impediment to information sharing nor liability protection to private sector entities for information sharing-related activities.

Cyber Security Framework

- The Order tasks the National Institute of Standards (NIST) with developing a Cybersecurity Framework, which "shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks."
- The Order directs the Framework to "incorporate voluntary consensus standards and industry best practices to the fullest extent possible."

Cyber Security Framework

- The Framework will also incorporate "guidance" for performance metrics to assess implementation by private entities.
- NIST is required to publish a preliminary version of the Framework within 240 days of the Order, and the final version will be published within one year of the Order.

Cyber Security Program

- The Order tasks the Secretary of Homeland Security, in coordination with sector-specific agencies, with establishing "a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities."
- The Secretary of Homeland Security is required to "coordinate establishment of a set of incentives designed to promote participation in the Program."

Other Agency Actions

- The Order requires agencies with authority for regulating the security of critical infrastructure to determine the adequacy of current cyber security regulations, in light of the preliminary Framework.
- If current regulations are deemed inadequate, within 90 days of publication of the final Framework, these agencies must propose proper actions to "mitigate cyber risk."

Actions by Independent Agencies

- The Order encourages independent regulatory agencies with the authority for regulating the security of critical infrastructure "to consider prioritized actions to mitigate cyber risks," in consultation with relevant agencies and "other affected parties."

Executive Order

- Will be implemented over 12-18 months
- Focuses on critical infrastructure
- Creates new security framework for businesses to implement (likely based on existing standards, but TBD)
- Required for some, voluntary for others
- Will likely create standard of care for businesses regardless of legal obligation to implement

Federal Legislation Under Construction

Into the Breach
MANAGING CYBER SECURITY THREATS IN THE DIGITAL AGE

Senate

- Critical infrastructure regulation
- Federal authorities
- Supply chain
- Information sharing
- National PII data breach standard?
- More breach disclosure requirements through SEC regulation?
- Hack back?

House

- Information sharing
- Federal authorities
- Supply chain
- National PII data breach standard?
- Hack back?

GOOD HARBOR SECURITY RISK MANAGEMENT, LLC

MAYER·BROWN

Cyber Disclosure Obligations for Public Companies

Into the Breach
MANAGING CYBER SECURITY THREATS IN THE DIGITAL AGE

In October 2011, the SEC issued guidance describing legal obligations to disclose material 1) cyber risks and 2) cyber incidents. This applies the longstanding legal requirement to disclose material information to investors in the context of cyber security.

Determining whether your company has experienced a material event – and building a cyber risk management program designed to reduce the likelihood of a material event – is a critical step for General Counsels and corporations

REUTERS

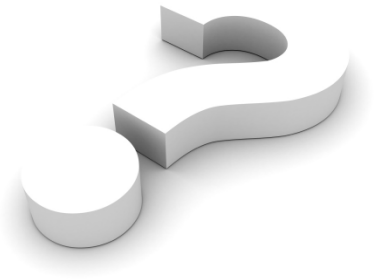
Hacked Companies Still Not Telling Investors
February 2, 2012

"At least a half-dozen major U.S. companies whose computers have been infiltrated by cyber criminals or international spies have not admitted to the incidents despite new guidance from securities regulators urging such disclosures."

GOOD HARBOR SECURITY RISK MANAGEMENT, LLC

MAYER·BROWN

QUESTIONS?



MAYER·BROWN

GOOD HARBOR
SECURITY RISK MANAGEMENT, LLC

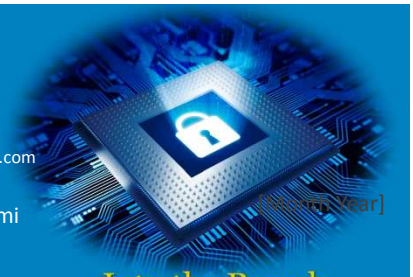
Cyber Vulnerabilities: Identifying Legal Risk and Approaches for Risk Mitigation

Larry Collins
Vice President E-Solutions,
Zurich Services Corporation
+1 917 453 2020
larry.collins@zurichna.com

Rebecca Eisner
Partner
Mayer Brown
+1 312 701 8577
reisner@mayerbrown.com

Jonathan Cooperman
Vice President and Assistant General Counsel , ACE North America
jonathan.cooperman@acegroup.com

Archis Parasharami
Partner
Mayer Brown
+1 202 263 3328
aparasharami@mayerbrown.com



What are the risks?

- This morning's message: The threat is real.
- Government regulators may investigate or bring actions:
  - DOJ
  - FTC
  - SEC
  - State AGs
- Plaintiffs' lawyers
  - Privacy class actions
  - Securities lawsuits
- Publicity / public relations

FTC "Red Flags" Rule

- Financial institutions and creditors covered
- Required to implement written Identity Theft Prevention Program (and updated)
  - Identify "red flag" patterns and practices of activity signaling possible identity theft
  - Use business practices to detect potential red flags
  - Plan response to red flag
- Cyber security breach affecting covered institution will likely result in investigation

Privacy class actions

- Even before cyber security threat, privacy class actions have been a growth area for plaintiffs' lawyers
- Plaintiffs invoke a wide variety of statutory and common-law theories (most of which pre-date the Internet age).
- Many lawsuits fail for lack of standing or lack of damages recognized under the law
- But such class actions threaten to impose substantial e-discovery costs and reputational harms

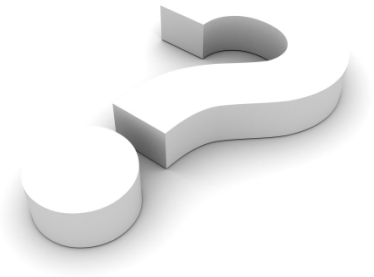
Private securities litigation

- Securities class action under Securities Exchange Act of 1934 (Rule 10b-5)
  - Alleged failure to disclose material information (existence of cyber security breach)
- Derivative suits against directors and officers
  - Alleged breach of fiduciary duty for failure to guard against breaches
- Likelihood of lawsuits succeeding seems (relatively) low, but potential costs imposed by such litigation could be tremendous

Risk mitigation strategies

- Legal and IT audits
- Instant response to data breach
- Insurance products
- Litigation defense (including privacy policies and dispute-resolution agreements)

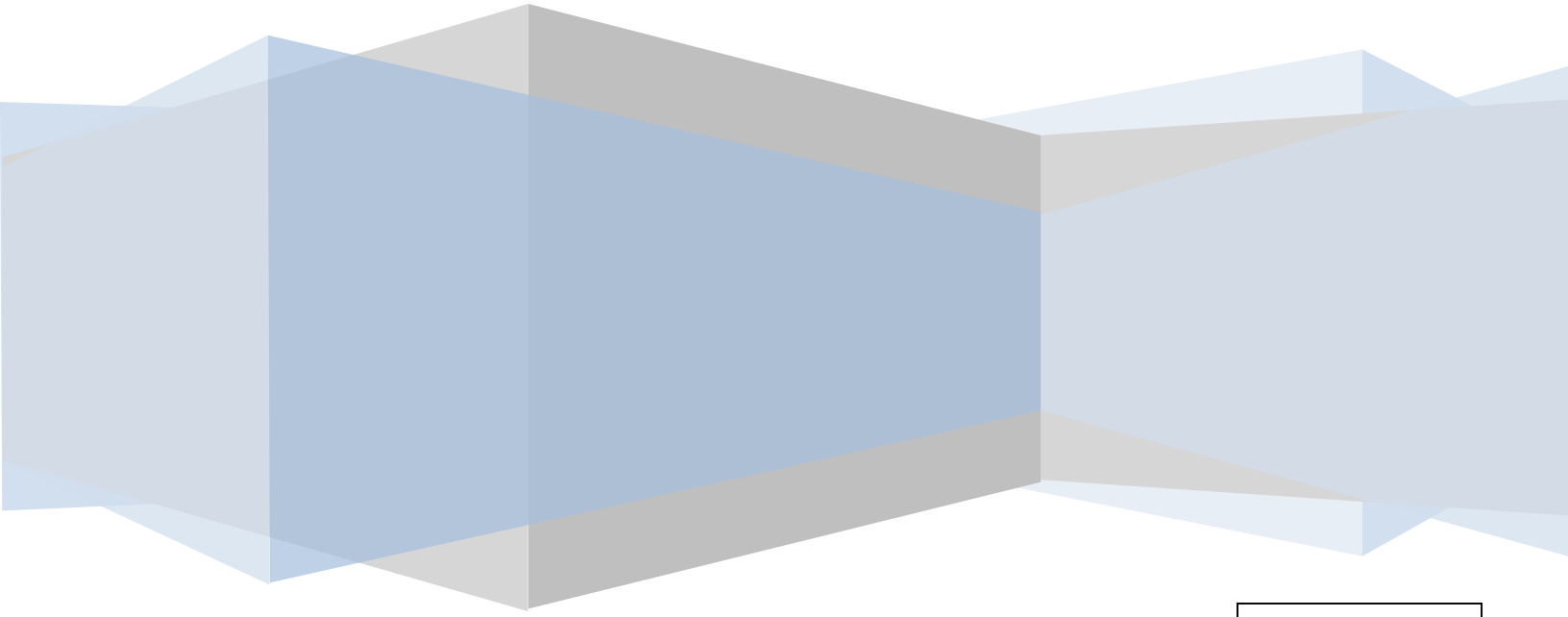
QUESTIONS?



Zurich North America

The Privacy Principles

Best practice in Information privacy



Larry Collins

June 6, 2012

Introduction

The attached principles are an excerpt from a document produced by the Organization for Economic Cooperation and Development entitled "*Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data."* The have become a major source of inspiration for laws and regulations governing information privacy, both here and the world over.

The Privacy Principles

1. Collection Limitation Principle

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

2. Data Quality Principle

Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

3. Purpose Specification Principle

The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

4. Use Limitation Principle

Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 3 except:

a) with the consent of the data subject; or

b) by the authority of law.

5. Security Safeguards Principle

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

6. Openness Principle

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal

The particular excerpt here comes from OECDprivacy.org and Mr. Ben Gerber . The site can be accessed by clicking on the "OECDprivacy.org link or by pasting the following URL into your browser - http://oecdprivacy.org.

data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

7. Individual Participation Principle

An individual should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him

i) within a reasonable time;
ii) at a charge, if any, that is not excessive;
iii) in a reasonable manner; and
iv) in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

8. Accountability Principle

A data controller should be accountable for complying with measures which give effect to the principles stated above.

The particular excerpt here comes from OECDprivacy.org and Mr. Ben Gerber . The site can be accessed by clicking on the "OECDprivacy.org link or by pasting the following URL into your browser - http://oecdprivacy.org.

Into the Breach

MANAGING CYBER SECURITY THREATS IN THE DIGITAL AGE

Presenter Bios

Richard Ben-Veniste
Partner
Mayer Brown
+1 202 263 3333
rben-veniste@mayerbrown.com

Richard Ben-Veniste is a highly respected litigator who focuses on complex civil litigation and white collar criminal cases. He also advises organizations and individuals involved in congressional investigations across a broad range of complex and sensitive areas.

Richard first achieved national prominence during the mid-1970s, when he served as one of the lead prosecutors on the Watergate Special Prosecution Force. Recognized as both a knowledgeable and experienced counselor and as a skilled and accomplished trial lawyer, he has been a key figure in some of the nation's most significant governmental activities at the intersection of law and politics.

Richard Clarke
Former National Coordinator for Security, Infrastructure Protection, and Counter-terrorism for the US and Current Chairman & CEO
Good Harbor Security Risk
+1 703 945 1307
rclarke@goodharbor.net

Richard A. Clarke is the Chairman of Good Harbor Security Risk Management, a consulting firm that works with senior corporate executives to assess and develop strategic cybersecurity programs that mitigate organizational risk in the face of advanced cyber threats. He is the author of Cyber War: The Next Threat to National Security and What to Do About It. He served as Special Advisor to Presidents Clinton and Bush (43) on Cybersecurity. Prior to that he was the White House's National Coordinator for Security, Counter-terrorism, and Critical Infrastructure.

Mr. Clarke served in national security positions in seven administrations, in the Pentagon, the State Department, the Intelligence Community, and an unprecedented ten consecutive years in the White House serving three Presidents.

Since leaving government, he has published five books (including the national #1 best seller, *Against All Enemies: Inside America's War on Terror*), taught for five years at Harvard's Kennedy School of Government, and serves as an on air consultant for ABC News.

Larry Collins
Vice President E-Solutions
Zurich Services Corporation
+1 917 453 2020
Larry.Collins@zurichna.com

Larry has more than 35 years of experience in Risk Engineering. As the Vice President of E-Solutions, he leads a team that provides electronic services to tens of thousands of on-line customers. He has appeared on TV on cyber security, spoken on a number of panels and published several articles and white papers on Security and Privacy related risk issues. He has also done many media interviews on that subject.

Larry's team recently received the Arthur Quern Quality Awards from the Risk and Insurance Managers Society (RIMS) for their Accident Review Tool. The Arthur Quern Quality Award recognizes significant contributions within the field of risk management that raises the quality of products, processes, programs, systems and services. The recipient of the Arthur Quern Quality Award demonstrates innovation within the risk management industry and increased quality in products, services and enterprise risk management within an organization.

Jonathan Cooperman
Vice President & Assistant General Counsel
ACE USA
jonathan.cooperman@acegroup.com

Jonathan Cooperman was appointed Vice President/Assistant General Counsel for ACE USA in 2008. He counsels underwriters in ACE's Professional Risk and Surety divisions, handling insurance policy drafting and negotiations for ACE's Digital Technology and Privacy Liability insurance products.

Mr. Cooperman has over 25 years of insurance experience, 16 years as an attorney. Prior positions include insurance coverage litigation associate with McKissock and Hoffman, Philadelphia, PA, and Claims Counsel for Philadelphia Insurance Companies.

Mr. Cooperman holds a B.A. degree from Vassar College, an M.B.A. from New York University, a J.D. from Temple University, and the C.P.C.U. and R.P.L.U. insurance designations.

Rebecca Eisner
Partner
Mayer Brown
+1 312 701 8577
reisner@mayerbrown.com

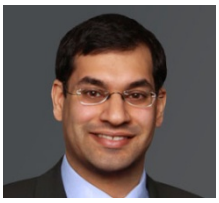
Rebecca is a partner in the Business & Technology Sourcing practice in the Chicago office. Rebecca focuses her practice on business and technology sourcing and outsourcing, information technology transactions, privacy and security. She has represented clients in complex global and offshore technology and business process outsourcing transactions, including information technology, procurement, finance and accounting, human resources, customer relationship and call centers, and development and transformational outsourcing. Rebecca regularly advises clients in data transfer and privacy issues affecting corporate initiatives, such as divestitures, global data programs, electronic contracting and signatures, web site design and review, CAN SPAM compliance, data breach notices to affected individuals, as well as emerging US security and privacy legal standards.

Jake Olcott
Principal
Good Harbor Security Risk Management
+1 703 945 1307
jacob.olcott@goodharbor.net

Jacob Olcott manages the Cybersecurity practice at Good Harbor, where he helps senior corporate executives, investment professionals, and government leaders develop programs that identify and mitigate cyber risk. Prior to joining Good Harbor, Mr. Olcott served as counsel to Senator John D. Rockefeller, IV, Chairman of the Senate Committee on Commerce, Science, and Transportation, where he acted as the Chairman's lead negotiator on comprehensive cybersecurity legislation. He also led a review of corporate disclosure practices that contributed to the issuance of groundbreaking cybersecurity guidance by the Securities and Exchange Commission in October 2011.

Mr. Olcott is the recipient of multiple awards during his time in Congress, including the Federal 100 Award for leaders in federal government information technology, the SANS Institute National SCADA Security Leadership Award, and the SANS Institute National Cybersecurity Policy Award.

Mr. Olcott holds a J.D. from the University of Virginia and a B.A. in History from the University of Texas at Austin.



Archis Parasharami
Partner
Mayer Brown
+1 202 263 3328
aparasharami@mayerbrown.com

Archis Parasharami, a litigation partner in Mayer Brown's Washington DC office, is a co-chair of the firm's Consumer Litigation & Class Actions practice, recently named by *Law360* as one of the top five class action groups of the year. He also is a member of the firm's Supreme Court & Appellate practice. Archis routinely defends businesses in class action litigation in federal and state courts around the country. He brings substantial experience to all aspects of complex litigation and class actions, with a particular focus on strategy issues, multidistrict litigation, and critical motions seeking the dismissal of class actions or opposing class certification. He also has helped businesses achieve settlements on highly favorable terms in significant class actions.

Philip Recht
Partner
Mayer Brown
+1 213 229 9512
precht@mayerbrown.com

Partner in charge of Mayer Brown's Los Angeles office and leader of the firm's California Government and Global Trade Practice group, Phil Recht represents clients in legislative, regulatory, enforcement and litigation matters before and involving federal, state and local governments. He also handles grants, approvals, permits and other government transactions. He has particular experience in transportation, tribal gaming, health care, trade association, government contracts, and election law matters.

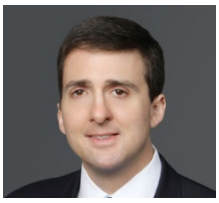
Richard Rosenfeld
Partner
Mayer Brown
+1 202 263 3130
rrosenfeld@mayerbrown.com

Richard M. Rosenfeld is co-lead of Mayer Brown's US Securities Litigation & Enforcement group working from both the Washington, DC and New York offices.

Richard has nearly 17 years of experience practicing in the securities field, including more than a decade in government regulatory and enforcement positions. Most recently, he was asked to return to the government from private practice in the midst of the financial crisis to serve as Chief Investigative Counsel in the Office of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP).

Jeffrey Taft
Partner
Mayer Brown
+1 202 263 3293
jtaft@mayerbrown.com

Jeffrey Taft is a partner in the Financial Services Regulatory and Enforcement (FSRE) practice in the Washington, DC office. He has extensive experience representing banks, bank holding companies, trust companies and other financial service providers on regulatory matters, including privacy and data security matters under the Gramm-Leach Bliley (GLB) Act, Fair Credit Reporting Act (FCRA), state privacy and data breach laws and anti-money laundering laws. He has assisted numerous clients with the creation and implementation of privacy and information security programs under the GLB Act and state privacy laws. He also regularly counsels clients on matters pertaining to the FCRA including its requirements for "firm offers" of credit, red flag guidelines and sharing information with affiliates.



Howard Waltzman
Partner
Mayer Brown
+1 202 263 3848
hwaltzman@mayerbrown.com

Howard Waltzman focuses his practice on communications and Internet law and commercial transactions in the United States and other key international markets. He represents some of the nation's leading communications service providers, manufacturers, and trade associations in regulatory and legislative matters, including with respect to privacy, cyber-security, Internet services, spectrum policy, and video programming. He also represents investors on these and other communications-related matters.

With respect to privacy, Howard's compliance work has included location-based services, CALEA, CAN-SPAM, and the Telephone Consumer Protection Act. He has also been involved in the Congressional debate surrounding online consumer privacy, data security, and cyber-security legislation.