Challenges In Compliance And Corporate Governance

Twelfth Annual Webcast

January 20, 2016

F. Joseph Warin
Alexander H. Southwell
Adam M. Smith

Scott D. Hammond
Lori Zyskowski
Sarah E. Fortt

GIBSON DUNN

Beijing • Brussels • Century City • Dallas • Denver • Dubai • Hong Kong • London • Los Angeles • Munich
New York • Orange County • Palo Alto • Paris • San Francisco • São Paulo • Singapore • Washington, D.C.

MCLE Certificate Information

- This program has been approved for credit in accordance with the requirements of the New York State Continuing Legal Education Board for a maximum of 2.0 credit hours, of which 2.0 credit hours may be applied toward the areas of professional practice requirement. This course is approved for transitional/non-transitional credit.
- Gibson, Dunn & Crutcher LLP certifies that this activity has been approved for MCLE credit by the State Bar of California in the amount of 2.0 hours.
- Gibson, Dunn & Crutcher LLP is authorized by the Solicitors Regulation Authority to provide in-house CPD training. This program is approved for CPD Credit in the amount of 2.0 hours. Regulated by the Solicitors Regulation Authority (Number 324652).
- Application for approval is pending with the Texas, Virginia, and Washington State Bars.
- Most participants should anticipate receiving their certificates of attendance via e-mail in approximately 4 weeks following the webcast.
- Members of the Virginia Bar should anticipate receiving the applicable certification forms in approximately 6 weeks.
- MCLE questions can be directed to Jeanine McKeown (National Training Administrator) at 213-229-7140 or jmckeown@gibsondunn.com.

Presentation Overview

- The Current Environment
- U.S. Regulatory & Enforcement Trends
- International Regulatory & Enforcement Trends
- Building & Overseeing Effective Compliance

The Current Environment

An Uncertain Landscape

Top Five Areas of Compliance Uncertainty and Risk

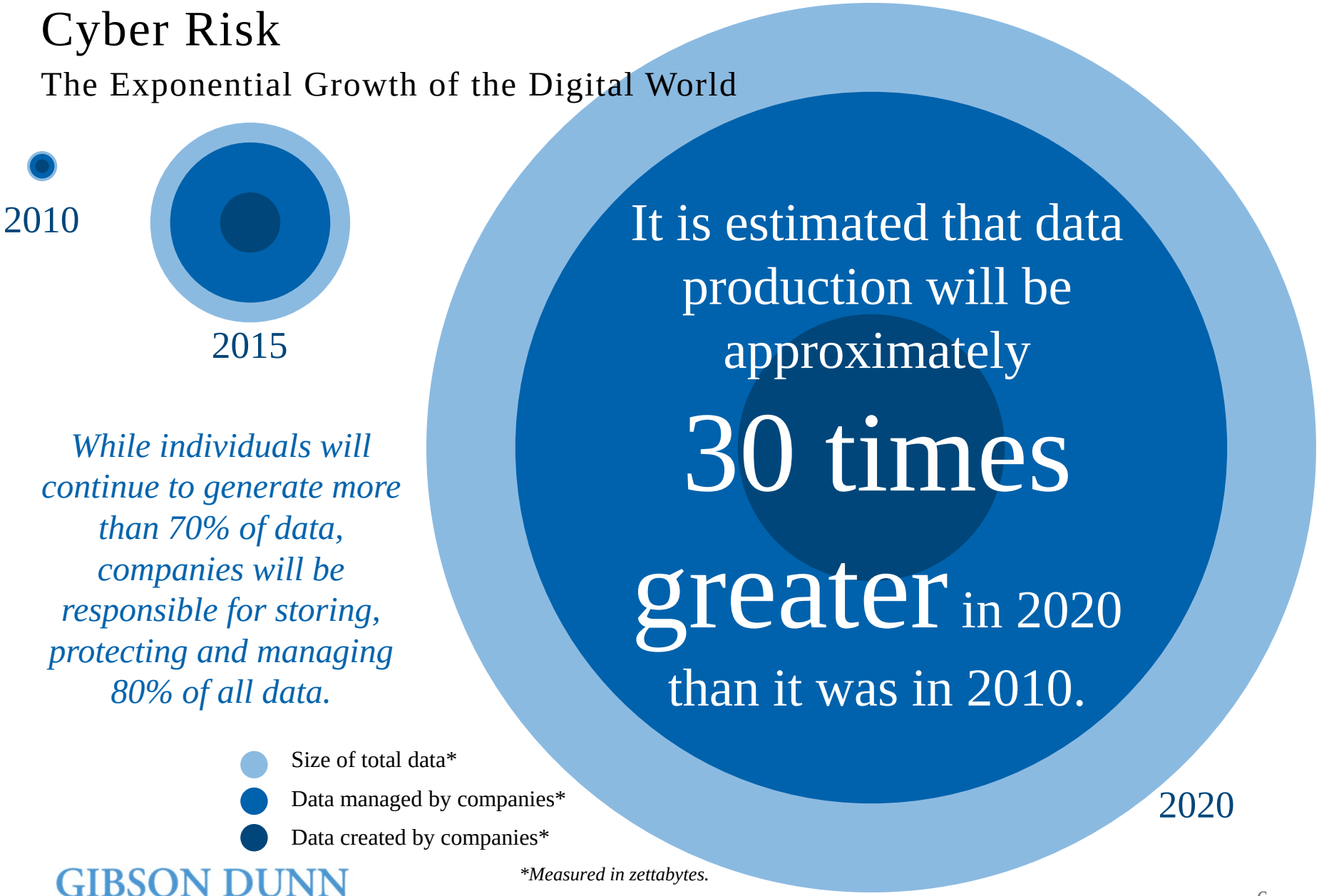
- Cyber Risk
- The New Activism
- Global Enforcement
- Individual Liability
- Regulatory Change

"The environment you work in is more complex than ever . . . . In fact, it is this complexity and speed of change that makes your jobs so important and renders it imperative that you consistently challenge yourself to evolve to meet the demands of your profession."

- Andrew J. Donohue, SEC Chief of Staff (Oct. 14, 2015)

Cyber Risk

The Exponential Growth of the Digital World



While individuals will continue to generate more than 70% of data, companies will be responsible for storing, protecting and managing 80% of all data.

- Size of total data*
- Data managed by companies*
- Data created by companies*

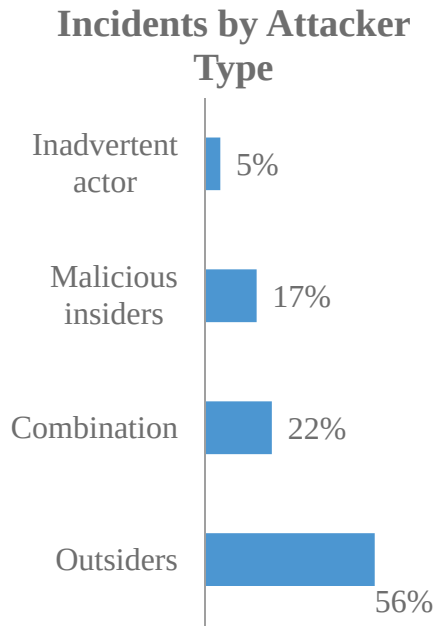
**Measured in zettabytes.*

GIBSON DUNN

1: The History of Data Breaches, Digital Guardian, Nate Lord (Sept. 28, 2015); CSC report (2014).

Cyber Risk

Acknowledging the Risk



The Risks from Cyberattack:

- **Lost Customers/Revenue**
- **Damage to Reputation/Brand**
- **Diverted Management and Board Focus**
- **Direct Response Costs**
- **Regulatory Investigations and Penalties**
- **Consumer Class Action Litigation**
- **Derivative Suits**
- **Shareholder Suits**

GIBSON DUNN

Corporate Board Member – Law in the Boardroom Study (2015), Figure 1
IBM Cyber Security Intelligence Index 2014, Figure 2

Cyber Risk

Identifying the Threat

Cyber risks are only getting more varied and complex.

The accident

- In 2015, the personal information of over 3 million Hello Kitty enthusiasts, including many children, was found to be vulnerable.

The homegrown threat

- A recent survey[1] found that one in seven employees would be willing to sell his/her corporate password, some for as little as $150.

The third-party risk

- In 2015, a data breach at PNI Digital Media, a small Canadian company, compromised the photo databases at CVS.
- In 2015, Chinese hackers exposed the information of more than 21.5 million U.S. government employees.

The global war

- In December 2014, BBC News reported that hackers had, for only the second known time ever, caused physical damage by cyber attack. The attackers had infiltrated a German steel mill through "spear-phishing" emails to override control systems and cause massive damage via the facility's blast furnace.

GIBSON DUNN

1: SailPoint Survey (Jan. 2015).

Cyber Risk

Identifying the Threat

- In November 2015, the U.S. Department of Justice ("DOJ") announced charges stemming from massive network intrusions at U.S. financial institutions, brokerage firms, and major news publications. DOJ alleged that three defendants had masterminded a "cybercriminal enterprise" with transnational scope which allegedly stole the personal information of over 100 million people.
    - According to Manhattan U.S. Attorney Preet Bharara, the personal information of over 80 million victims was stolen from a single financial institution. Mr. Bharara described the alleged scheme as representing a "new world of hacking for profit" "to support a diversified criminal conglomerate"—"hacking as a business model." According to DOJ, this constitutes the largest theft of customer data from a U.S. financial institution in history.
- In April 2015, a multinational telecommunications corporation agreed to pay $25 million to the Federal Communications Commission ("FCC") to settle investigations into data privacy breaches at the company's call centers in Mexico, Colombia, and the Philippines. These breaches resulted in the alleged disclosure of personal data for almost 280,000 of the company's customers.
- A recent survey[1] of public company board members found that 55% of director respondents believe that a board is never fully able to address all of the risks in the current corporate environment, and a majority see technology risks, such as cyber and social media risk, as especially challenging.
- According to a U.S. Army War College study, the People's Liberation Army is "preparing for total cyber warfare."[2]

1: NYSE Corporate Board Member Survey (Q1 2015).
2: Information as Power: China's Cyber Power and America's National Security, Colonel Jayson M. Spade (2011).

Cyber Risk

Identifying the Threat: Supply Chain

- Supply chain risk is a particular area of concern—especially for companies that plan to expand into new geographies—and another area that requires collaboration with the compliance function.
  - Supplier or third-party compliance has risen rapidly as a top future perceived risk, with 22% of respondents to a recent survey[1] placing it among their top three future risks—double the percentage who gave it that ranking in 2014.
  - Despite the growing threat of supplier problems, the same survey indicates that supply chain personnel are represented on compliance committees only 13% of the time—a minimal gain over last year's 12%.

1: 2015 PWC State of Compliance Survey.

The New Activism

As of the end of 2014, activist funds worldwide had approximately $237 billion worth of stock holdings

In 2015, approximately 22% of companies targeted by activists were either mid- or large-cap companies

In 2015, activist investors made 707 new investments in North America alone

- ***Performance is no longer a defense***. 1/3 of targets outperformed their peers in the 12 months preceding an activist attack.
- ***Size is no longer a defense***. Since January 2011, there were over 75 instances of activist campaigns targeting companies with $10 billion+ in market capitalization.
  - DuPont, Dow Chemical, HP, PepsiCo, Microsoft, P&G, and BNY Mellon—all over $40 billion.
- ***Economic activism often piggybacks on governance activism***. Governance issues offer "levers" for activists to compel events at target companies, and governance activism has made economic activism more effective (*e.g.*, by eroding takeover defenses).

Source: Activist Insight

Rising International Enforcement

The Balance Tips Towards Global Action

- 2015 continued the trend of increased international enforcement, with transnational bribery prosecutions by foreign authorities taking center stage.
  - ***Brazil***: Prosecutors involved in investigating the sprawling corruption scandal at Petrobras, the state-owned oil company, having already charged 173 individuals with corruption- and bribery-related offenses, have announced that they will soon expand their focus to foreign contractors.
  - ***China***: In November 2015, as part of China's anti-corruption campaign, "Operation Sky Net," the country enacted the Ninth Amendment to the PRC Criminal Law. The amendment allows for greater punishments for those who offer and give bribes.
  - ***U.K.***: In November 2015, the FCA fined Barclays plc £72 million for engaging in a transaction with ultra-high net worth clients which raised "unacceptable" bribery and economic crime risk.
- The increasingly aggressive international approach is coupled with a rise in intergovernmental cooperation, which raises the stakes for multinational corporations.

Increasingly, robust global enforcement efforts mean that companies are best served by implementing a multifaceted compliance program that emphasizes more than FCPA risk.

Rising International Enforcement

"Quadruple Dipping"

- Increasingly, international violations—and focus from enforcement agencies in multiple jurisdictions—mean that companies are often penalized many times over for alleged conduct centering on the same core facts.
- Example: RBS—LIBOR and FX Resolutions:

	FX	LIBOR	Collateral Class Action
	**DOJ**: $395 million **Fed**: $274 million **CFTC**: $290 million	**DOJ**: $150 million **CFTC**: $325 million	$225 million
	**FCA**: $344 million	**FCA**: $137 million	
		**EC**: $530.2 million	

GIBSON DUNN

13

Individual Liability

- In the U.S., DOJ's Yates Memorandum issued in September 2015 (and discussed further below) may signal an expansion of the Department's pursuit of individuals for corporate wrongdoing.

In the last couple of years, compliance officers at a number of large, international companies have been fined, banned, suspended, or asked to leave.

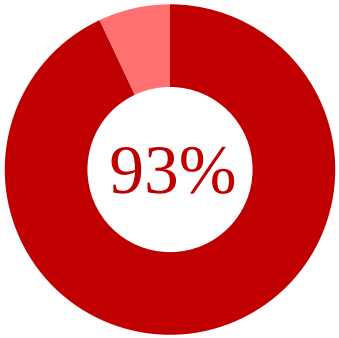
- Across the pond in the U.K., the new Senior Managers and Certified Persons Regime will require banks and other financial institutions to allocate certain responsibilities to individuals and document the accountabilities (beginning in March 2016).
- There is concern among some that this requirement will allow regulators to bring more actions against individuals in the future.

Individual Liability

"In my experience, in the enforcement arena, the most effective deterrent is strong enforcement against responsible individuals, especially senior executives. In the end, it is people, not institutions, who engage in unlawful conduct."
– Mary Jo White, SEC Chair (Mar. 12, 2015)

"At your annual meeting two years ago, Chair White addressed the potential liability of compliance professionals for securities law violations. She said that compliance officers should not fear enforcement action if they perform their responsibilities diligently, in good faith, and in compliance with the law. That is still true today."
– Andrew Ceresney, SEC Director of Enforcement (Nov. 4, 2015)

- A recent Thomson Reuters study[1] finds that regulators are increasingly targeting individuals rather than firms, and compliance professionals are concerned that they will be the focus of accountability. Based on the Thomson Reuters' survey, there is a widespread expectation that this shift in regulatory focus towards senior leadership will increase and extend internationally.



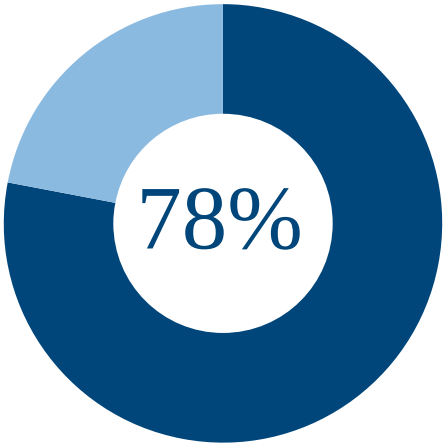
of compliance professionals expect the personal liability of compliance professionals to increase in the next year (64% expect a significant increase).[1]

GIBSON DUNN

1: Thomson Reuters Report on Personal Liability (2015).

Regulatory and Governance Developments

- The 2014-2015 proxy season brought a wave of proxy access proposals, and proxy access adoptions are occurring on a weekly basis.
- Counseling ~50 clients on over 150 shareholder proposals submitted for 2015 meetings, Gibson Dunn has historically submitted more than one of every four no-action request letters filed with the SEC regarding shareholder proposals.



- 2015 brought a significant number of proposed and final rules, regulations, and guidance impacting governance practices and disclosure.

78% of CEOs around the world view increasing regulation as the top threat to business growth.[1]

- In addition, despite the U.S. Securities and Exchange Commission's ("SEC") disclosure effectiveness initiative, the Commission has added to companies' disclosure burden over the past few years, and continues to do so pursuant to the Dodd-Frank mandate.

1: 2015 PWC State of Compliance Survey.

2015 Global Regulatory Summary

- ***Europe***
  - In December 2015, the European Commission, Parliament, and Council of Ministers reached agreement on the General Data Protection Regulation ("GDPR"). When it receives final approval, the GDPR will establish a single set of data protection rules to apply across Europe (including to non-EU companies operating in the EU).
  - The U.K. Consumer Rights Act introduced collective actions for damages claims before the Competition Appeals Tribunal ("CAT") and empowered the CAT to hear standalone claims before a violation is proven.
- ***China***: China introduced key changes into law demonstrating the intent to prosecute the supply side of bribery. The amendments, effective November 1, 2015, prohibit offering bribes to current and former state functionaries, as well as those persons closely related to them, and impose monetary fines on individual defendants.
- ***Brazil***: In March 2015, Brazil enacted legislation implementing the Clean Company Act, which had been in effect since January 2014. The new legislation establishes guidelines for the calculation of corporate fines, sets forth the requirements for corporate leniency agreements, and provides the framework for evaluating corporate compliance programs.

U.S. Regulatory & Enforcement Trends

U.S. Regulatory & Enforcement Trends

- 2015[1] DOJ and SEC Enforcement Summaries and Policy Updates
- Updates on Key Enforcement and Regulatory Topics:
  - U.S. Trade Sanctions
  - Antitrust
  - Foreign Corrupt Practices Act ("FCPA")
  - False Claims Act ("FCA")
  - Consumer Financial Protection Bureau ("CFPB")
  - Commodity Futures Trading Commission ("CFTC")
  - Financial Institutions Reform, Recovery, and Enforcement Act ("FIRREA")
  - Criminal Tax
  - Virtual Currency Update
  - Governance and Other Key Developments

1: Statistics and information set forth for DOJ, SEC and other U.S. governmental bodies are based on the U.S. government's fiscal year, which runs from October 1st of the prior year. through September 30th of the applicable year.

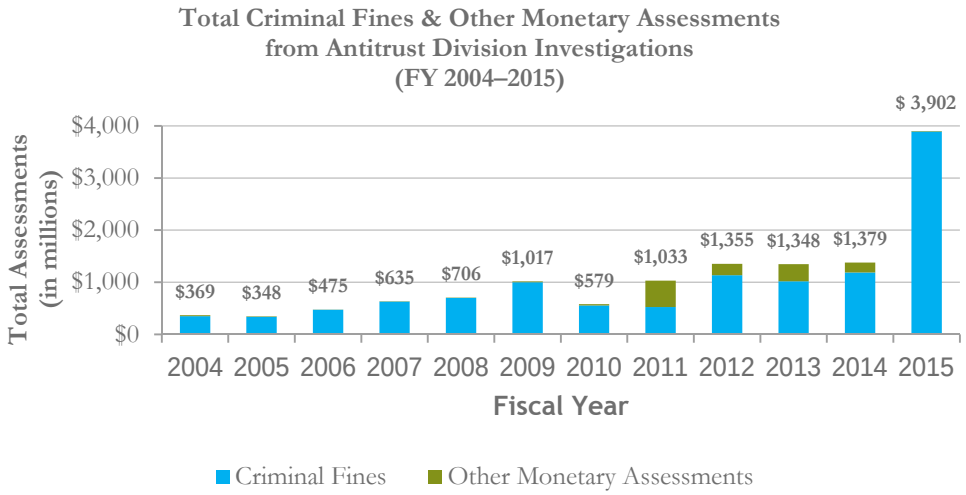
Details on DOJ Enforcement in 2015

Key 2015 Developments

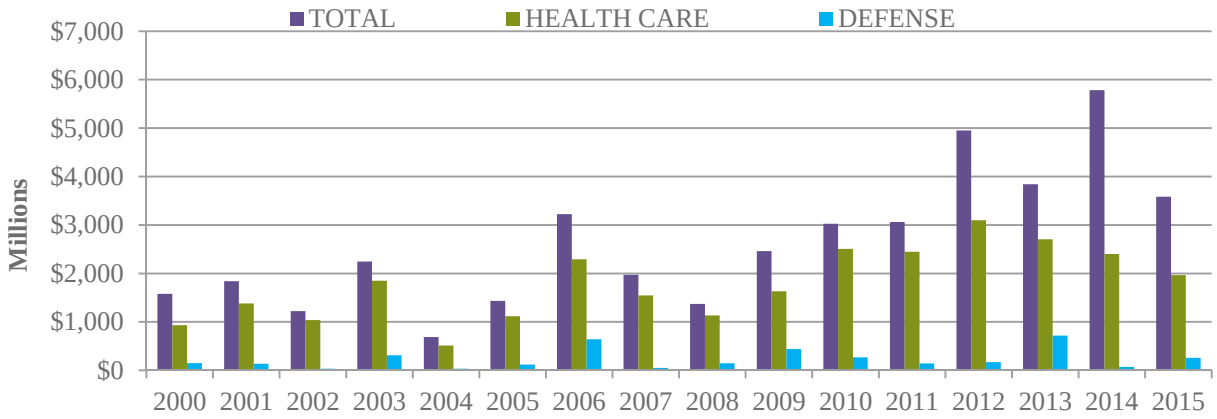
- In December 2014, the Second Circuit vacated the convictions of insider trading defendants Anthony Chiasson and Todd Newman. The Second Circuit held that the government must prove both that (1) the tippee knew that an insider disclosed confidential information, and (2) the tippee knew the tipper did so in exchange for a personal benefit. On October 5, 2015, the Supreme Court declined to review the case.
- As part of a wide-ranging investigation that has attracted global attention, DOJ has charged 41 defendants for their role in a decades-long kickback scheme involving the Fédération Internationale de Football Association ("FIFA"). Twelve individuals and two marketing agencies have pleaded guilty.
- In June 2015, the Second Circuit affirmed the bank and wire fraud convictions of three former securities traders, upholding DOJ's use of FIRREA—and its ten-year statute of limitations—because the fraud exposed the company to criminal penalties and, therefore, "affected a financial institution."

DOJ Fines and Recoveries Remain High

- DOJ obtained approximately $3.9 billion in criminal fines for violations of the Sherman Act—another all-time high.
- Over 70% of that total resulted from the nearly $2.8 billion paid by various banks in DOJ's ongoing investigation into the manipulation of certain foreign exchange rates.



Annual FCA Recoveries by Industry



- At $3.6 billion in 2015, FCA settlements and judgments moved downward slightly from the almost $5.7 billion reported in 2014.

GIBSON DUNN

DOJ Enforcement Priorities

Based on recent statements by DOJ officials, DOJ 2015-2016 priorities include:

- ***Increased international cooperation***, including coordination with overseas counterparts to prosecute crimes in multiple jurisdictions;
- ***FCPA enforcement***, including the addition of three new white collar squads focusing primarily on the FCPA (in NY, DC, and a "virtual squad"), and of ten new prosecutors, which will increase the number of dedicated FCPA staff to 35; and
- ***Evaluation of corporate compliance and internal controls***, including the recent hire of dedicated compliance counsel, Hui Chen, to better evaluate companies' claims about their compliance programs.

"We are seeking to assure that companies have tough but realistic compliance programs that detect and deter individual wrongdoing by executives. Importantly, our compliance counsel will be instrumental in ferreting out whether a corporate compliance program is truly effective, or a mere paper tiger."

– Andrew Weissmann, Chief, DOJ Fraud Section
(July 30, 2015)

DPA/NPA Policy Update

- 2015 was a record-breaking year for DPAs and NPAs, with DOJ and the SEC entering into 100 agreements (more than double the previous high of 40 agreements, set in 2010). The huge increase in DPAs and NPAs is largely due to the DOJ Tax Swiss Bank Program, which resulted in 75 NPAs over the course of 2015.
- In November 2015, SEC Enforcement Director Andrew Ceresney announced a new threshold requirement for companies hoping to secure a NPAs or DPAs. Ceresney stated that only those companies who self-report the misconduct in question will be eligible for these alternative resolution vehicles.
- In May 2015, DOJ announced the revocation of a company's 2012 NPA, marking "the first time in recent history that the Department of Justice has found that a company breached an NPA over the objection of the company."[1]
- In April 2015, Senator Elizabeth Warren of Massachusetts criticized DPAs and NPAs as "get-out-of-jail-free cards," arguing that they do not provide a meaningful deterrent effect and suggesting that they allow companies to evade the criminal justice system.

1: Loretta Lynch, U.S. Att'y Gen., Remarks at a Press Conference on Foreign Exchange Spot Market Manipulation (May 20, 2015).

DOJ Emphasizes Individual Accountability

In September 2015, DOJ issued a new policy memorandum, known as the Yates Memorandum, outlining "six key steps to strengthen [DOJ's] pursuit of individual corporate wrongdoing":

- in order to qualify for any cooperation credit, corporations must provide DOJ all relevant facts relating to the individuals responsible for the misconduct;
- criminal and civil corporate investigations should focus on individuals from the beginning of the investigation;
- criminal and civil attorneys handling corporate investigations should be in routine communication with each another;
- absent extraordinary circumstances or approval, DOJ will not release culpable individuals from civil or criminal liability when resolving a matter with a corporation;
- DOJ attorneys should not resolve matters with a corporation without a clear plan to resolve related individual cases, and should memorialize any declinations as to individuals in such cases; and
- civil attorneys should consistently focus on individuals as well as the company and evaluate whether to bring suit against an individual based on considerations beyond that individual's ability to pay.

DOJ Emphasizes Individual Accountability

- On November 16, 2015, DOJ announced revisions to the USAM in accordance with the policy shift outlined in the Yates Memorandum.
  - The revisions reiterate the need for prosecutors to focus on individual wrongdoing throughout the course of their investigations, describing individual accountability as one of the "foundational principles of corporate prosecution," and making the disclosure of "all non-privileged information about individual wrongdoing" a threshold requirement for companies to receive any cooperation credit.

"Only by seeking to hold individuals accountable in view of all of the factors [in the Yates Memorandum] can the Department ensure that it is doing everything in its power to minimize corporate fraud and, over the course of time, minimize losses to the public fisc through fraud."
– Sally Quillian Yates, Deputy Attorney General
(Sept. 9, 2015)

Details on SEC Enforcement in 2015

Key 2015 Developments

- As of the end of 2015, the SEC announced that it brought 807 enforcement actions and obtained orders totaling approximately $4.2 billion in disgorgement and penalties in 2015. This was an increase from 2014, in which the SEC filed 755 enforcement actions and obtained orders totaling $4.16 billion.

The SEC's 2015 enforcement efforts were marked by:

- Holding "gatekeepers"—lawyers, accountants, and other functions tasked with ensuring corporate compliance—accountable for "failures to comply with professional standards";
- Pursuing novel theories, for example:
  - Hiring practices cases in the FCPA context (*e.g.*, BNY Mellon);
  - Instituting settled proceedings against advisers for their alleged failure to adequately disclose monitoring fees;
- Demanding that defendants make admissions of wrongdoing to achieve settlement;
- Increased focus on certain industries, including financial institutions; and
- Regarding the "broken windows" policy, the debate continued during the SEC's Investor Advisory Committee Meeting in October 2015.

SEC Enforcement Priorities

Based on recent statements by SEC officials,[1] SEC 2015-2016 priorities include:

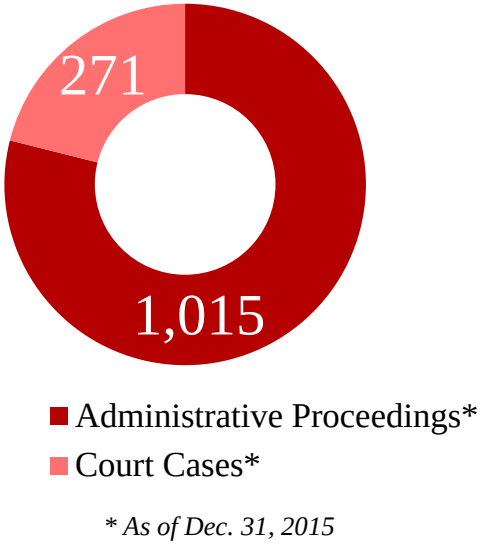
- ***Private equity issues***, including undisclosed conflicts of interest, misallocation of fees and expenses, and failure of controls;
- ***Financial fraud***, including faulty valuations, insufficient disclosures, and misrepresentation of performance;
- ***Self-reporting,*** including requiring companies voluntarily to disclose violations to be eligible for DPAs or NPAs; and
- ***Individuals and gatekeepers***, including cases against senior executives and compliance officers who fail to design and/or implement controls sufficient to prevent foreseeable misconduct.

"Vigorous and comprehensive enforcement protects investors and reassures them that our financial markets operate with integrity and transparency, and the Commission continues that enforcement approach by bringing innovative cases holding executives and companies accountable for their wrongdoing sending clear warnings to would-be violators."
– Mary Jo White, SEC Chair
(Oct. 22, 2015)

1: SEC&DOJ Hot Topics 2016 Panel – New York, New York (Nov. 12, 2015).

Preference for Administrative Proceedings Continues

- As we discussed in last year's webcast, the SEC faced criticism—including from Judge Jed Rakoff (S.D.N.Y.)—regarding the SEC's preference for administrative proceedings over federal court. Rakoff expressed concerns about the "administrative fiat" and "administrative creep" of the agency's internal enforcement power.
- In September 2015, the SEC announced proposed amendments to rules governing its administrative proceedings. These included:



** As of Dec. 31, 2015*

"Our litigators have also had a string of successes in administrative proceedings."

– Andrew Ceresney, SEC Director of Enforcement (May 12, 2015)

- A slight extension of the administrative proceeding schedule;
- Limited discovery for respondents;
- The exclusion of some unreliable evidence;
- A streamlined appeal process;
- Discretionary deadlines on Commission decisions; and
- A requirement for electronic submissions.

SEC Targets Cybersecurity

- Two recent speeches, one by Chair White and one by Chief of Staff Donohue, have highlighted the need for compliance professionals to familiarize themselves with the SEC's cybersecurity guidance.
- The SEC recently settled its enforcement action against investment adviser R.T. Jones Capital Equities Management for "stor[ing] sensitive personal identifiable information … without adopting written policies and procedures regarding the security and confidentiality of that information and protection of that information from anticipated threats."[1]

"The Commission has brought, and will continue to bring, enforcement actions against compliance officers when appropriate."

– Andrew J. Donohue, SEC Chief of Staff

(Oct. 14, 2015)

"While cybersecurity attacks cannot be entirely eliminated, it is incumbent upon private fund advisers to employ robust, state-of-the-art plans to prevent, detect, and respond to such intrusions."

– Mary Jo White, SEC Chair

(Oct. 16, 2015)

- The Commission also recently announced a second round of examinations of broker-dealers and investment advisers. These examinations will include, among other things, information on cybersecurity responsibilities.
- Early in 2015, the SEC Division of Investment Management released guidance on the measures that funds and advisers should consider in addressing cybersecurity risk.

1: In the Matter of R.T. Jones Capital Equities Management, Inc. (Sept. 22, 2015).

Cyber Regulation Developments

"Because the threats we face are blurring the lines between lone hackers and nation states, and between criminal and national security threats, we are facing a changing world order in which lone hackers, organized crime syndicates and nation states are all increasingly able to harm our shared networks and our livelihood."

– Assistant Attorney General John P. Carlin (Sept. 30, 2015)

- In April 2015, President Obama declared cyber threats to be a "national emergency." He signed an executive order authorizing the U.S. Treasury to impose financial sanctions on entities that "create a significant threat to U.S. national security, foreign policy, or [the] economic health or financial stability of the United States" through cyber attacks.
- During his recent State of the Union address, President Obama emphasized the importance of protecting our economy from cyber terrorism.
- In March, the New York Department of Financial Services ("NY DFS") issued new guidance on appropriate cyber security practices, stating that "all institutions [should] view cyber security as an integral aspect of their overall risk management strategy, rather than solely as a subset of information technology," and asserting that NY DFS would incorporate cyber security topics into its existing IT examination framework.[1]
- In August, the Third Circuit upheld the Federal Trade Commission's ("FTC") ability to bring enforcement actions over data breaches as an "unfair" practice under Section 5 of the FTC Act, denying a challenge brought by Wyndham Worldwide Corp. to the agency's jurisdiction. The FTC's guidance on appropriate cybersecurity practices was cited as an authority by the court.[2]

1: http://www.dfs.ny.gov/about/letters/ltr150326_cyber.pdf

2: *F.T.C. v. Wyndham Worldwide Corp.*, No. 14-3514, 2015 WL 4998121 (3d Cir. Aug. 24, 2015).

Cyber Regulation Developments

- On December 18, 2015, Congress passed the Cybersecurity Act of 2015 as part of the Consolidated Appropriations Act.
- The Cybersecurity Act provides a framework for non-federal entities and federal entities to voluntarily share cybersecurity information with each other.
- The Cybersecurity Act requires the Director of National Intelligence, the Secretaries of Defense and Homeland Security, and the Attorney General to develop procedures for the sharing of "cyber threat indicators" and defensive measures.
- Private entities that participate will receive antitrust and other liability protections. Participation will not constitute a waiver of any legal protections, including legally protected trade secrets, and the information shared will be exempt from FOIA and other disclosure laws. However, once shared, information may be used by federal entities for: (1) responding to, preventing, or mitigating a specific and serious threat; (2) responding to, investigating, prosecuting, preventing, or mitigating a serious threat to a minor; or (3) preventing, investigating, disrupting, or prosecuting offenses arising from cyber-related criminal activities.

SEC Commissioners Express Concern Over Individual Liability

- There also has been criticism of the perceived increase in the prosecution of individuals. Notably, SEC Commissioner Gallagher voted against and spoke out condemning what he believed to be an SEC trend toward strict liability for compliance officers.
- Commissioner Aguilar, while disagreeing with Commissioner Gallagher about the existence of a trend toward stricter enforcement against compliance officers, released a statement seeking to reassure compliance officers that the SEC was not increasing enforcement against them.

"While I respect the views of my fellow commissioners, based on what I'm hearing from the CCO community [I am] . . . left [with] the impression that the SEC is taking too harsh of an enforcement stance against CCOs, and that CCOs are needlessly under siege from the SEC. Thus, I am concerned that the recent public dialogue may have unnecessarily created an environment of unwarranted fear in the CCO community. Such an environment is unhelpful…"

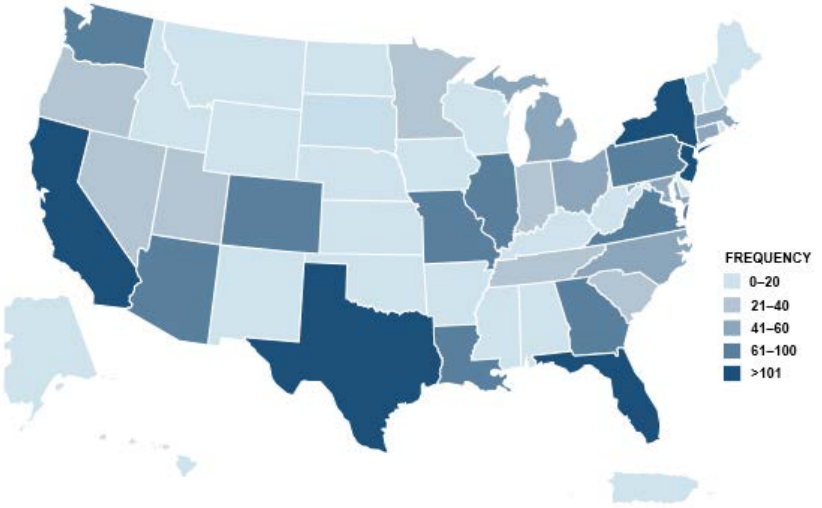
– Luis A. Aguilar, SEC Commissioner

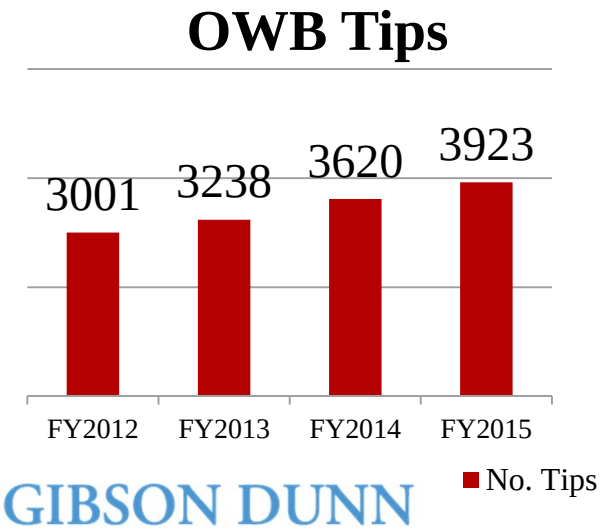
(June 2015)

Whistleblower Update[1]

2015 by the Numbers

- The SEC's Office of the Whistleblower ("OWB") received 3,923 whistleblower tips from all 50 states, the District of Columbia, and Puerto Rico, as well as 61 foreign nations.
- The SEC awarded approximately $38 million to eight whistleblowers.





- The most common complaints made by whistleblowers in 2015 related to corporate disclosures and financials (17.5%), offering fraud (15.6%), and market manipulation (12.3%).
- 186 tips related to alleged FCPA violations (4.7%), a 17% increase from 159 tips in 2014.

GIBSON DUNN

1: 2015 Annual Report to Congress on Dodd-Frank Whistleblower Program.

Whistleblower Update[1]

Notable Awards

""[I]t is past time to stop wringing our hands about whistleblowers. They provide an invaluable public service, and they should be supported."

– Mary Jo White, SEC Chair (April 30, 2015)

- In April 2015, the SEC brought its first Rule 21F-17(a) enforcement action against KBR for use of language in separation agreements that allegedly impeded whistleblower reports. The separation agreements prohibited witnesses in internal investigations from discussing topics with outside parties without advance authorization. There was no evidence that KBR ever enforced the provision; however, KBR paid a $130,000 penalty.
- In April 2015, the SEC awarded 30% of the sanctions to be collected in *In the Matter of Paradigm Capital Management, Inc. and Candace King Weir*, amounting to over $600,000, to a whistleblower who "suffered unique hardships," including allegedly unlawful retaliation, as a consequence of making the report. This was the first case filed by the SEC under its new authority to bring anti-retaliation enforcement actions.
- In November 2015, the SEC announced a whistleblower award totaling more than $325,000 for a former investment firm employee. The SEC's press release noted that the whistleblower waited to come forward until after leaving the firm, and stated that the award may have been higher had the whistleblower acted sooner.

1: 2015 Annual Report to Congress on Dodd-Frank Whistleblower Program.

Model Release Language

Example Only[1]

- ***Non-Interference with Protected Rights***. This Agreement and Release is not intended to interfere with Employee's exercise of any protected, nonwaivable right, including Employee's right to file a charge with, participate in an investigation by, or provide truthful information to the Equal Employment Opportunity Commission or other government agency. By entering into this Agreement and Release, however, Employee acknowledges that the consideration set forth herein is in full satisfaction and is inclusive of any and all amounts, including, but not limited to, attorneys' fees, to which Employee might be entitled or which may be claimed by Employee or on Employee's behalf against the Released Parties and Employee is forever discharging the Released Parties from any liability to Employee for any acts or omissions occurring on or before the date of Employee's signing of this Agreement and Release.

- ***Confidentiality of Agreement***. Employee agrees and promises not to disclose, either directly or indirectly, in any manner whatsoever, any information regarding the existence or terms of this Agreement and Release, to any person or entity, except to members of Employee's immediate family, Employee's attorney and Employee's accountant and/or financial adviser, *provided* that such persons agree to keep this information confidential, and except as may be required by law. Nothing herein shall prevent Employee or Employer from providing truthful information to governmental authorities or in response to a subpoena or discovery request.

1: This is only an example; companies should seek counsel in drafting and assessing release language..

DOJ/SEC Personnel Update

DOJ

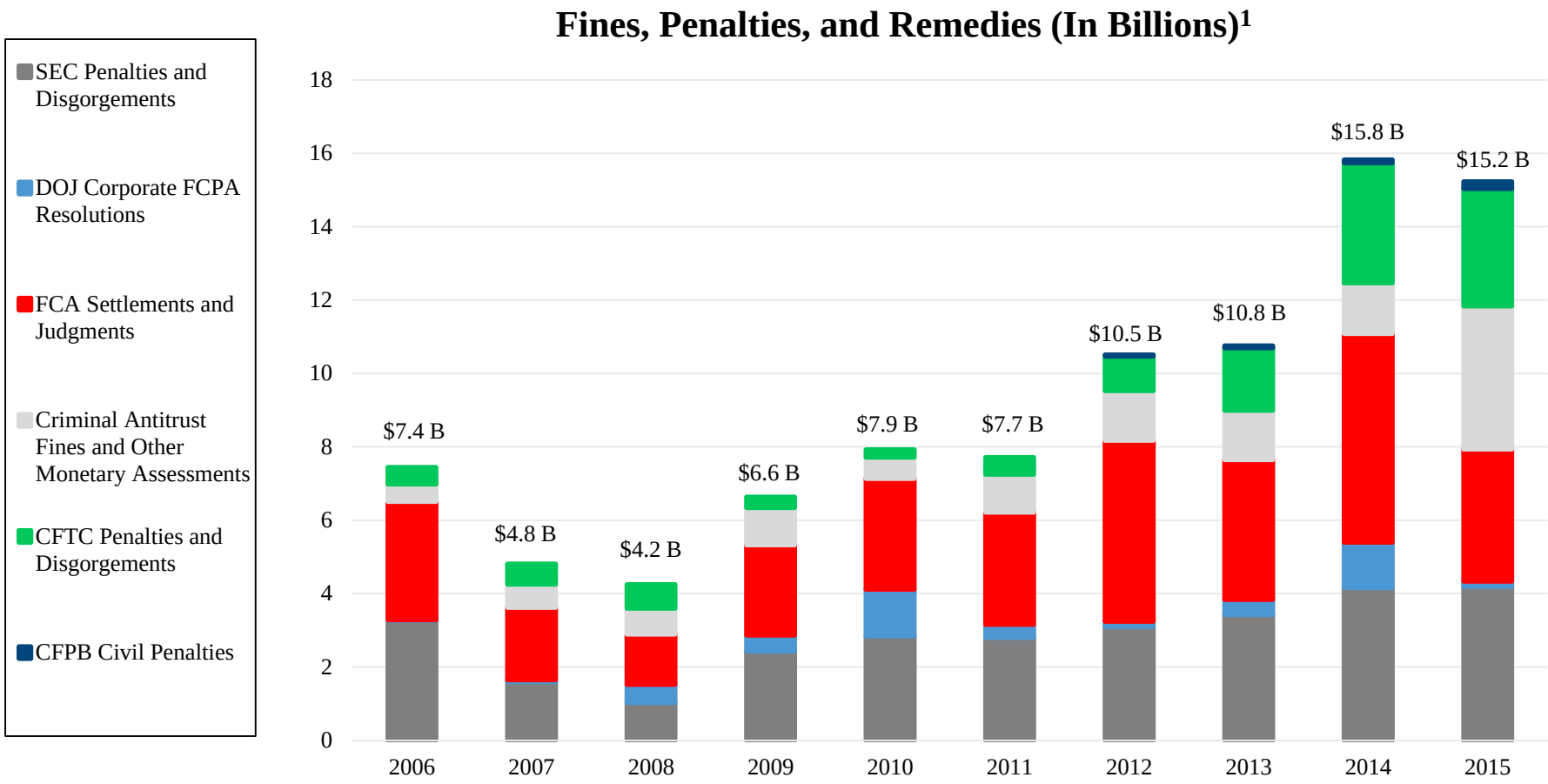
- DOJ has been significantly increasing its resources to focus on enforcement priorities. This includes adding:
  - A new compliance counsel to advise on whether companies should receive credit for the quality of their compliance programs in an enforcement action;
  - Ten new prosecutors to the FCPA unit, increasing its size by 50%; and
  - Three new squads to the FBI's International Corruption Unit, which focuses on FCPA and kleptocracy matters.
- In September 2015, DOJ announced plans to embed a prosecutor within the European Cybercrime Centre, which comes on the heels of the late 2014 creation of DOJ's Cybersecurity Unit.

SEC

- The White House has nominated Lisa Fairfax, George Washington University law professor, to replace SEC Commissioner Luis Aguilar, and Mercatus fellow, Hester Peirce, to replace SEC Commissioner Daniel Gallagher.

Updates on Key Enforcement and Regulatory Topics

U.S. Fines Remain High



While total fines in 2015 dipped slightly from 2014 due to lower FCPA and FCA fines, increased criminal antitrust fines and other monetary assessments augmented the decline.[1]

GIBSON DUNN

1: GDC Internal Aggregations. CFPB Civil Penalties does not include CFPB recoveries and restitutions. CFPB recoveries and restitutions were included in prior iterations of this graphic, but are now addressed below.

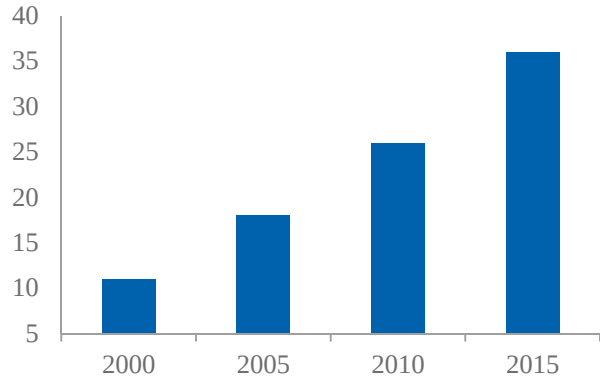
Top Fines, Records, and Penalties in 2015 for Anti-Corruption, Antitrust, FCA, and Sanctions Offenses

Amount	Industry/Company	Area	Date
$925M	A large U.S. based financial corporation	Foreign Exchange (DOJ)	May 2015
$800M	A large foreign financial institution	LIBOR (CFTC)	Apr. 2015
$775M	A large foreign financial institution	LIBOR (DOJ)	Apr. 2015
$710M	Barclays plc	Foreign Exchange (DOJ)	May 2015
$550M	JPMorgan Chase & Co.	Foreign Exchange (DOJ)	May 2015
$450M	A national kidney-dialysis company	False Claims Act	June 2015
$441M	Barclays plc	Foreign Exchange (FCA)	May 2015
$400M	Barclays plc	Foreign Exchange (CFTC)	May 2015
$395M	Royal Bank of Scotland plc	Foreign Exchange (DOJ)	May 2015
$330M	Crédit Agricole	Sanctions (OFAC)	Oct. 2015
$390M	A pharmaceutical company	False Claims Act	Nov. 2015
$385M	Crédit Agricole	Sanctions (NY DFS)	Oct. 2015
$342M	Barclays plc	Foreign Exchange (Fed)	May 2015
$342M	A large U.S. based financial corporation	Foreign Exchange (Fed)	May 2015
$342M	JPMorgan Chase & Co.	Foreign Exchange (Fed)	May 2015
$340M	A large foreign financial institution	LIBOR (FCA)	Apr. 2015
$312M	Crédit Agricole	Sanctions (state claims)	Oct. 2015

U.S. Economic and Trade Sanctions Update

- The U.S. continues to rely on economic sanctions as a primary tool of diplomacy and national security.
- New programs have been instituted very quickly, blacklisted entities have been added and removed at an unprecedented pace, and the number and severity of enforcement actions—at both the federal and state level—have increased remarkably.
  - Since 2000, the U.S. active sanctions programs have grown by 300%.
  - Since 2009, the number of individuals and entities on the "Specially-Designated Nationals" ("SDN") blacklist has increased by 40%.
  - The average annual rate of change to the SDN list has almost doubled since 2007.

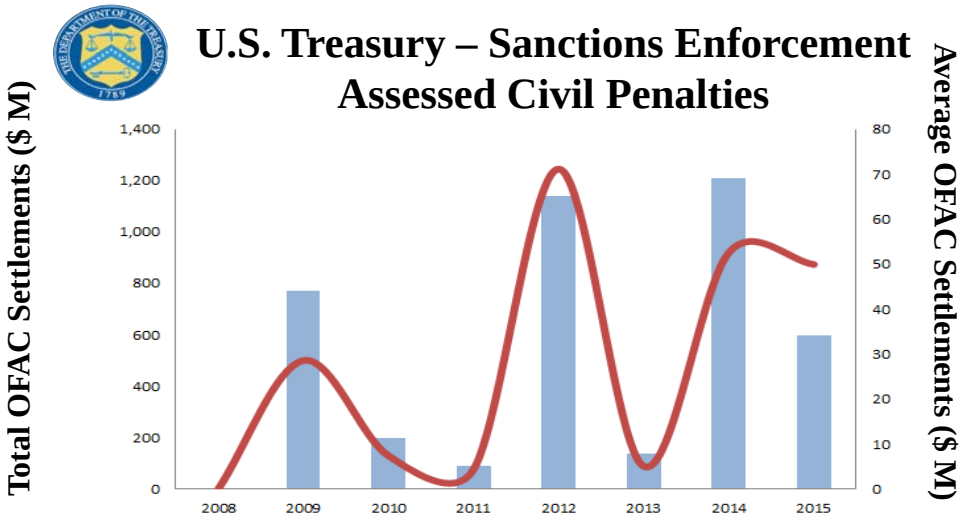
Active Sanctions Programs



OFAC Update

Recent Enforcement Cases

- Three major European financial institutions settled allegations of violating Iran, Sudan, Myanmar, Cuba, Terrorism, and/or Weapons Proliferation sanctions—fined $258 million, $1.7 million, and $330 million.

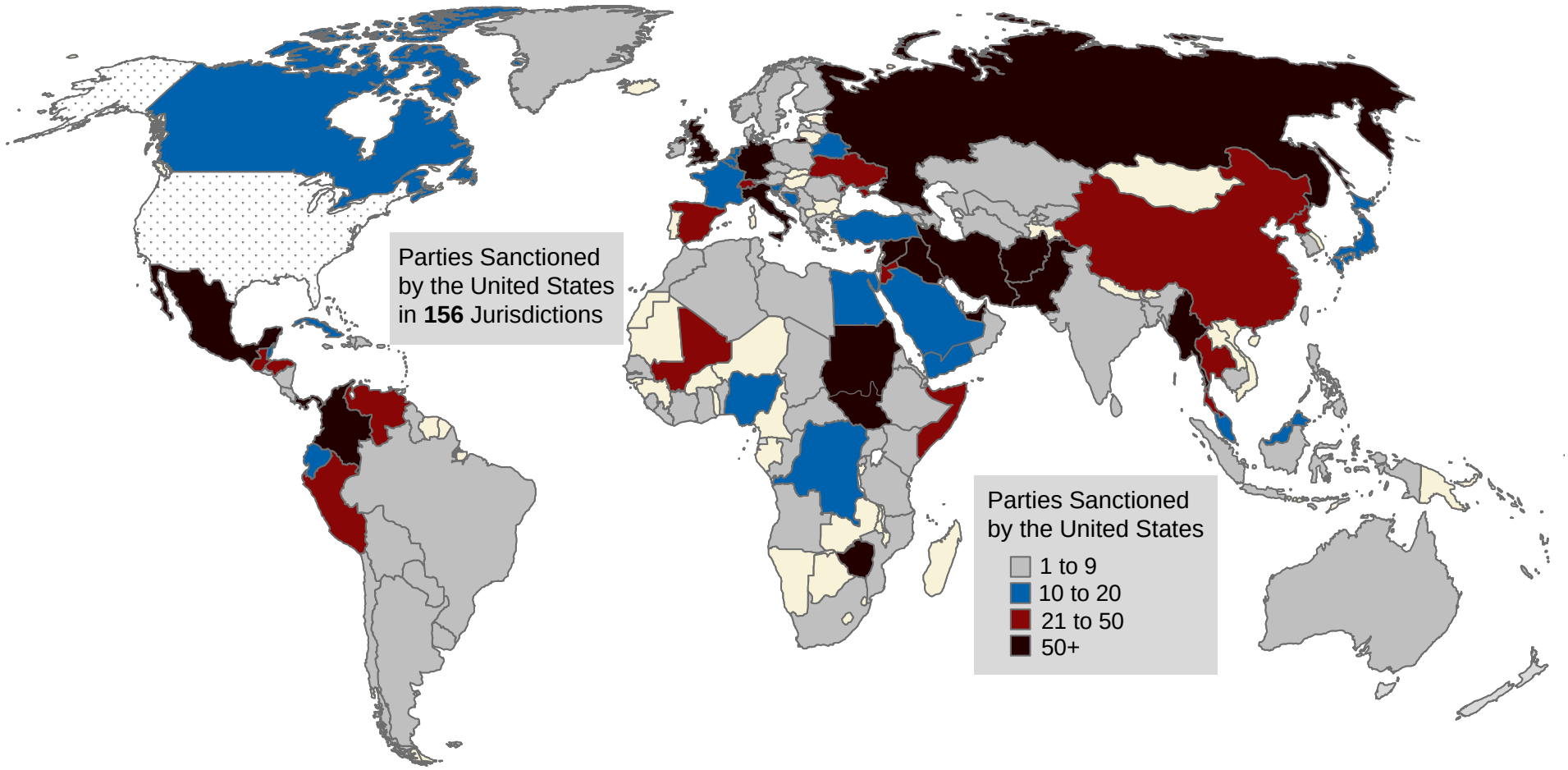


These fines are in addition to penalties and forfeitures assessed by other federal and state authorities including the Department of Justice, the Federal Reserve, the Office of the Comptroller of the Currency, the NY Department of Financial Services and the District Attorney of NY, which have regularly exceeded the amount and scope of penalties assessed by OFAC.

- The largest online payment processer settled accusations of violating Iran, Cuba, Sudan, Terrorism, and Weapons Proliferation sanctions—fined $7.6 million.
- A manufacturer settled allegations that it violated Weapons Proliferations sanctions—fined $390,000.
- A large non-governmental organization settled accusations of violating Iraq sanctions—fined $780,000.

GIBSON DUNN

U.S. Economic and Trade Sanctions Update



GIBSON DUNN

U.S. Sanctions

Current U.S. Sanctions Programs

Highly Active

1. Iran Gov't Blocking/ITSR/IFCA
2. Iran CISADA/IFSR
3. Ukraine/Russia
4. Transnational Criminal Organizations
5. North Korea
6. Syria
7. Counternarcotics/Kingpin
8. Counterterrorism
9. WMD
10. Foreign Sanctions Evaders (E.O. 13608)
11. Human Rights Violators via Information Technology (GHRAVITY: E.O. 13606)
12. Cuba
13. South Sudan

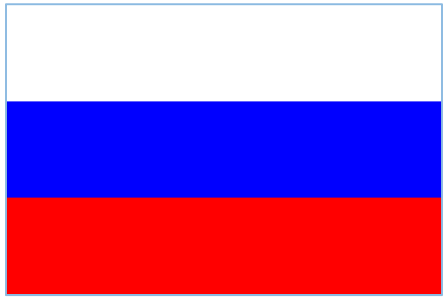
Moderately Active

14. Democratic Republic of the Congo
15. Central African Republic
16. Myanmar
17. Sudan
18. Zimbabwe
19. Somalia
20. ISA
21. Russia Human Rights (Magnitsky)

Less Active

22. Yemen
23. Belarus
24. Liberia
25. Cote d'Ivoire
26. Libya
27. Lebanon
28. Iraq
29. HEU Assets Control
30. Western Balkans
31. FTO
32. Rough Diamonds
33. Iran Assets Control (Hostages)
34. WMD Trade Control
35. Terrorism Sanctions 31 CFR 596
36. Terrorism List Gov'ts 31 CFR 596
37. Malicious Cyber-Enabled Activities
38. Burundi

U.S. Economic and Trade Sanctions Update: Russia, Cuba, Burma



- There are two principles guiding the U.S. response to President Putin's incursion into Ukraine:
  - Maximize impact on Russia while minimizing pain on allies and economy.
  - As far as possible, move "in lockstep" with closest allies and partners.
- Current sanctions target core drivers of the Russian economy in the finance, energy, and defense sectors, with complicate sanctions regulations; Crimea is essentially off-limits economically.

- In December 2014, President Obama announced "the most significant changes in [U.S.-Cuba] policy in more than fifty years."
- Summary of key sanctions relief to date: travel, exports, and imports (e.g., support for small businesses), entrepreneurial efforts (*e.g.*, establishing a commercial presence in Cuba), financial services (*e.g.*, opening accounts in Cuba), and other matters (*e.g.*, payment for certain legal services).

- Through a series of general licenses issued since 2012 and culminating in a license promulgated in December 2015 OFAC has now authorized: (1) exports of financial services to Burma, (2) imports of Burmese goods into the U.S. (except certain gemstones), (3) new investment in Burma (with reporting requirements to the Department of State), and (4) *most* transactions with four of the country's leading financial institutions and its major air- and seaports – all of which happen to be SDNs.

GIBSON DUNN

U.S. Economic and Trade Sanctions Update: Iran

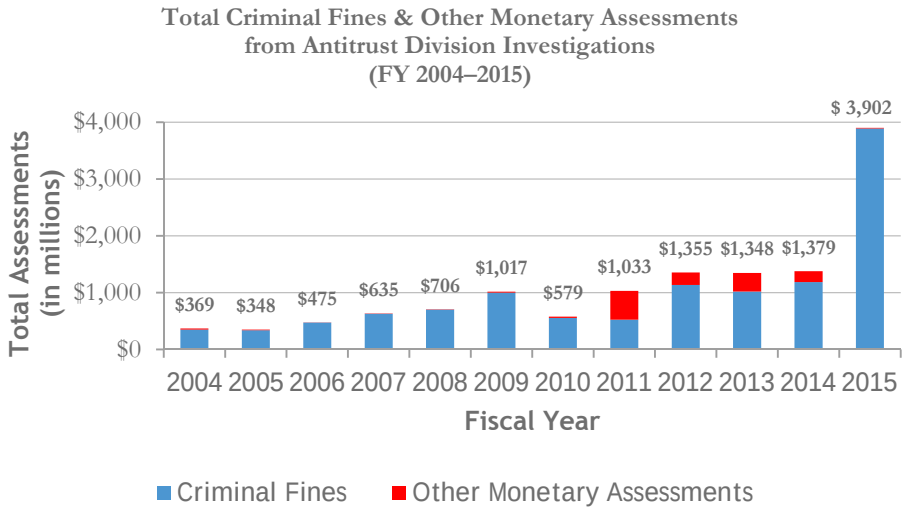
- On January 16, 2016 ("Implementation Day"), the comprehensive international sanctions that had restricted dealings with Iran and Iranian entities were substantially eased.
- Following Implementation Day, E.U. and UN sanctions have all broadly been eased; U.S. sanctions have not been.
- The broad U.S. embargo on Iran – barring access to the U.S. financial system for Iran and Iran-related business, and exports of U.S. goods and services to Iran – remains essentially untouched.
- The limited U.S. sanctions relief on offer is targeted and constrained. It includes the:
  - Lifting of "secondary sanctions," which prohibited non-U.S. firms from engaging with Iran – however, there are continued exceptions to this relief to certain Iranian entities, dealings with which still incur secondary sanctions exposure;
  - Potential for licenses for civil aviation sales into Iran, including of U.S. equipment – however, there are significant constraints regarding end-user restrictions and uncertain financing arrangements; and
  - Allowance for foreign subsidiaries of US parents to engage with Iran – however, only inasmuch as such engagement is consistent with the nuclear agreement and has almost no nexus with the United States.
- It is unclear whether the relief granted on Implementation Day will be sufficient for the private sector to take advantage of new openings in Iran – or if further relief will have to be provided.

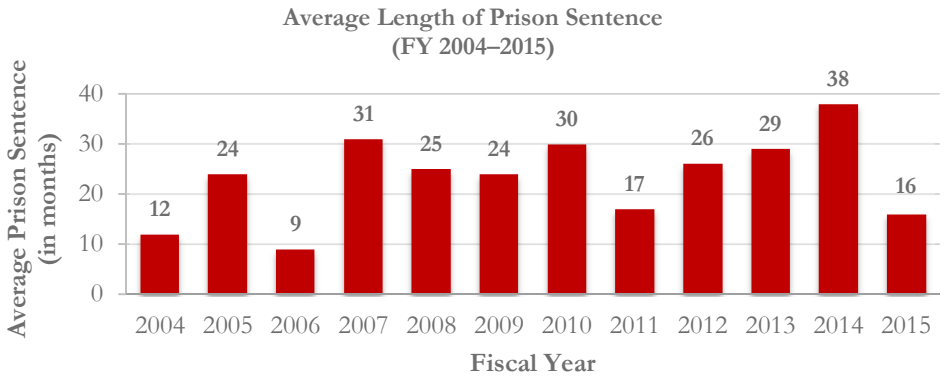
Antitrust Update

Fines

2015 Record Fines:

- The Antitrust Division has obtained approximately $3.9 billion in criminal fines for violations of the Sherman Act—an all-time high.
- Over 70% of that total, or approximately $2.8 billion, resulted from the foreign exchange rate-related guilty pleas by various banks.
- The $775 million that a large foreign financial institution agreed to pay for its role in allegedly manipulating certain LIBOR transactions contributed to the Division's record year.





GIBSON DUNN

Antitrust Update

Fines

- The fines have been substantial, but rather than simply gape at the gross volume of fines, the pertinent question remains whether global competition authorities will seek convergence in the methodologies used to calculate fines when sanctioning the same overarching conduct.
- Recently, U.S. Deputy Assistant Attorney General Brent Snyder indicated that while prosecutions could be brought, and thus penalties calculated, on the basis of foreign component sales where there are no direct sales of a price-fixed product into the United States, doing so increased the risk of duplicative sanctions under the increasingly robust global competition regime. DOJ has taken foreign penalties into account when negotiating the resolution of certain investigations.
- Against the backdrop of heightened anti-cartel enforcement comes a simple reminder that, in some cases, trial remains a viable and sensible strategy. 2015 brought acquittals in high-profile criminal antitrust trials in the U.S., Canada, and the U.K., including one in the Antitrust Division's long-running investigation concerning coastal water freight transportation between the United States and Puerto Rico.

Antitrust Update

Foreign Nationals Serving U.S. Prison Sentences

- Approximately 100 foreign nationals have served, or are currently serving, U.S. prison sentences for violating the U.S. antitrust laws and/or obstructing a DOJ Antitrust Division investigation.
- Since 2010, the average jail sentence for non-U.S. citizens in Antitrust Division cases is nearly 16 months (it is significantly longer for U.S. citizens).
- Nearly all of the jailed foreign nationals voluntarily submitted to U.S. jurisdiction, but the Antitrust Division has had recent success with extradition.
- Antitrust Division policy is to insist on recommending jail sentences for antitrust offenders, and it will not enter into a "no jail" plea agreement where it only recommends that an individual pay a fine.

Antitrust Update

Prison Sentences

Executives from these countries have been prosecuted by DOJ (Antitrust Division) for price fixing, bid rigging and customer and/or market allocation agreements:

- The United States
- Brazil
- Canada
- France
- Germany
- Italy
- Luxembourg
- The Netherlands
- Norway
- Sweden
- Switzerland
- United Kingdom
- Japan
- South Korea
- Taiwan
- New Zealand
- South Africa

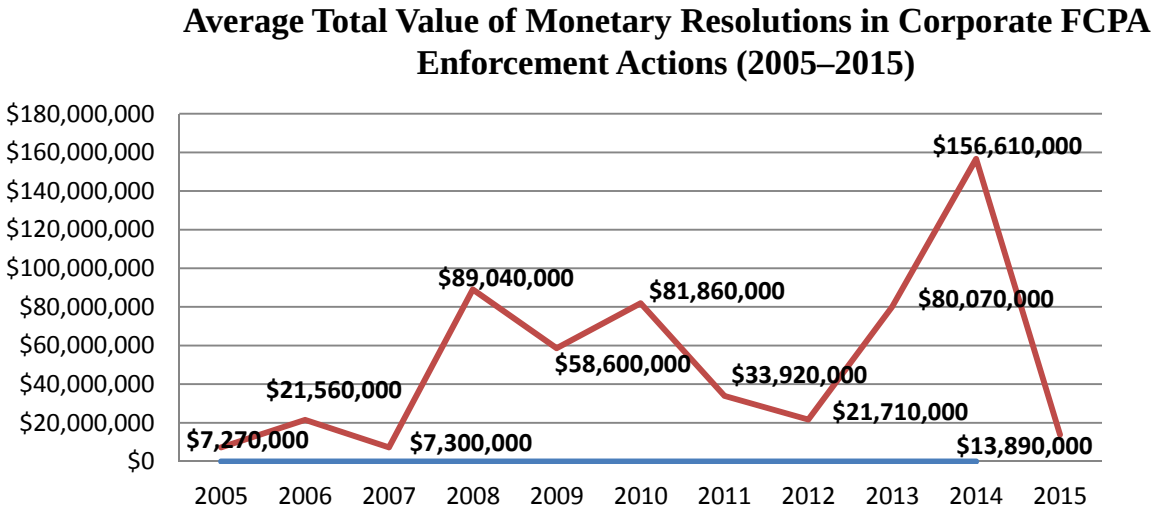
Executives from these countries have served prison sentences in the United States for violating the U.S. antitrust laws:

- The United States
- Canada
- France
- Germany
- Italy
- Luxembourg
- The Netherlands
- Norway
- Sweden
- Switzerland
- United Kingdom
- Japan
- South Korea
- Taiwan

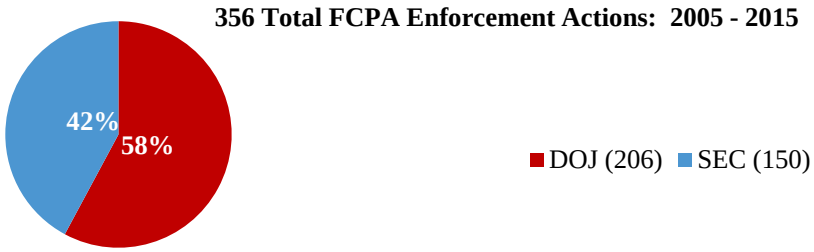
FCPA (SEC and DOJ) Statistics

2015 Fines and Penalties

- In 2015, DOJ initiated 2 FCPA corporate enforcement actions; the SEC initiated 8 such actions.
- The relatively greater number of corporate SEC actions during 2015 is consistent with DOJ's focus on individual wrongdoers and increasing use of declinations to encourage cooperation with criminal enforcement authorities.



The fines and penalties imposed for FCPA violations continue to be significant, demonstrating that foreign bribery may be too costly for business to bear.



FCPA (SEC and DOJ) Key Trends

Enforcement Partnerships

- DOJ and SEC are taking increasing advantage of government and non-government resources—*e.g.*, the FBI and whistleblowers—to more aggressively investigate suspected violations of the FCPA. FBI strategies include outreach to the private sector, partnerships with domestic and foreign agencies, training of vulnerable businesses, the formation of dedicated anti-corruption squads, and "proactive enterprise theory investigations" requiring covert surveillance.

Cross-Border Corruption Prosecutions

- U.S. enforcement authorities have made it a priority to engage their foreign counterparts when investigating foreign corruption and bribery. They have invested resources in providing assistance and training to foreign enforcement authorities, and these efforts already have resulted in coordinated global settlements. For example, a U.K. based bank agreed to pay a total of $36.9 million to settle actions with the SEC and the U.K.'s SFO.

FCPA (SEC and DOJ) Key Trends

SEC Enforcement

- Andrew Ceresney, the SEC's Director of Enforcement, announced that companies hoping to secure an NPA or DPA for FCPA violations will only be eligible if they voluntarily disclose potential misconduct to the SEC.
- The SEC increasingly is bringing standalone internal controls cases or standalone books and records cases, without bringing charges for bribery of government officials under Section 30A of the Securities Exchange Act.
- Although DOJ led the chart with respect to individual accountability in 2015, the SEC set the pace for corporate FCPA enforcement.
  - Eight of the ten corporate enforcement actions filed in 2015 were brought by the SEC.
  - Further, there were no joint DOJ-SEC FCPA prosecutions of companies in 2015, which is a stark departure from prior years in which it was more probable than not that a company subject to the jurisdiction of both agencies (corporate issuers) would resolve with both.

FCPA Monitorships

- Since 2004, 41 out of 129 corporate FCPA enforcement actions by the SEC and DOJ (32%) have resulted in the imposition of a compliance monitor.
  - Of those cases in which the defendant made a voluntary disclosure (73), a compliance monitor was imposed in 23 cases (32%).
  - Of those cases in which the defendant did not make a voluntary disclosure (56), a compliance monitor was imposed in 18 cases (32%).
- Of the 10 FCPA cases resolved in 2015, only one involved the imposition of a compliance monitor (Louis Berger International Inc.).

ISO Anti-Bribery Management Standard

- ISO is working on anti-bribery management systems standard ISO 37001 to assist small, medium, and large public and private sector organizations across the world to prevent bribery and promote ethical business cultures. The standard articulates specific anti-bribery measures and controls, including with regard to:
  - Tone from the top;
  - Due diligence on third parties;
  - Controls on gifts and hospitality; and
  - Confidential reporting procedures.

"ISO 37001 will help an organization comply with international anti-bribery good practice and legal requirements . . . . It will . . . ultimately provide a competitive advantage to organizations."

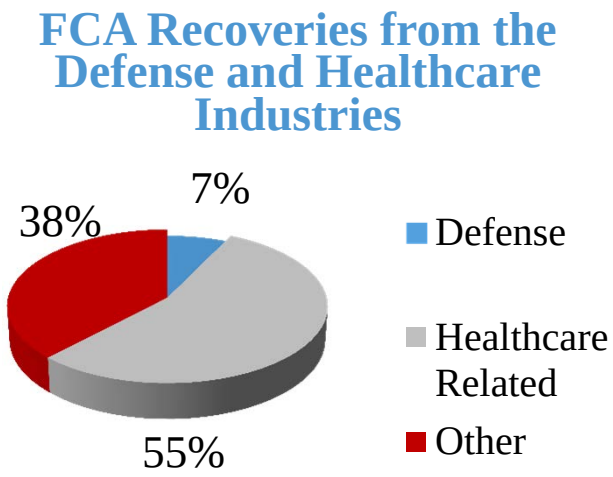
– Neill Stansbury, Chairman of ISO 37001 Committee

(May 27, 2015)

- The standard is currently at the Committee Draft Stage, and more than 80 experts from 44 countries are involved in its development.
- Finalization of the standard is expected by the end of 2016.

FCA Statistics and Key Trends

- ***2015 Statistics***
  - The healthcare industry provided the largest source of FCA settlements and judgments, with $1.966 million recovered by DOJ for healthcare fraud recoveries.
  - 2015 was the first year in several years without a single healthcare settlement exceeding $1 billion, demonstrating the broad scope of the government's enforcement efforts.
  - Recoveries from government contracting and defense-industry firms amounted to $1.1 billion, of which the highest single settlement was $146 million.

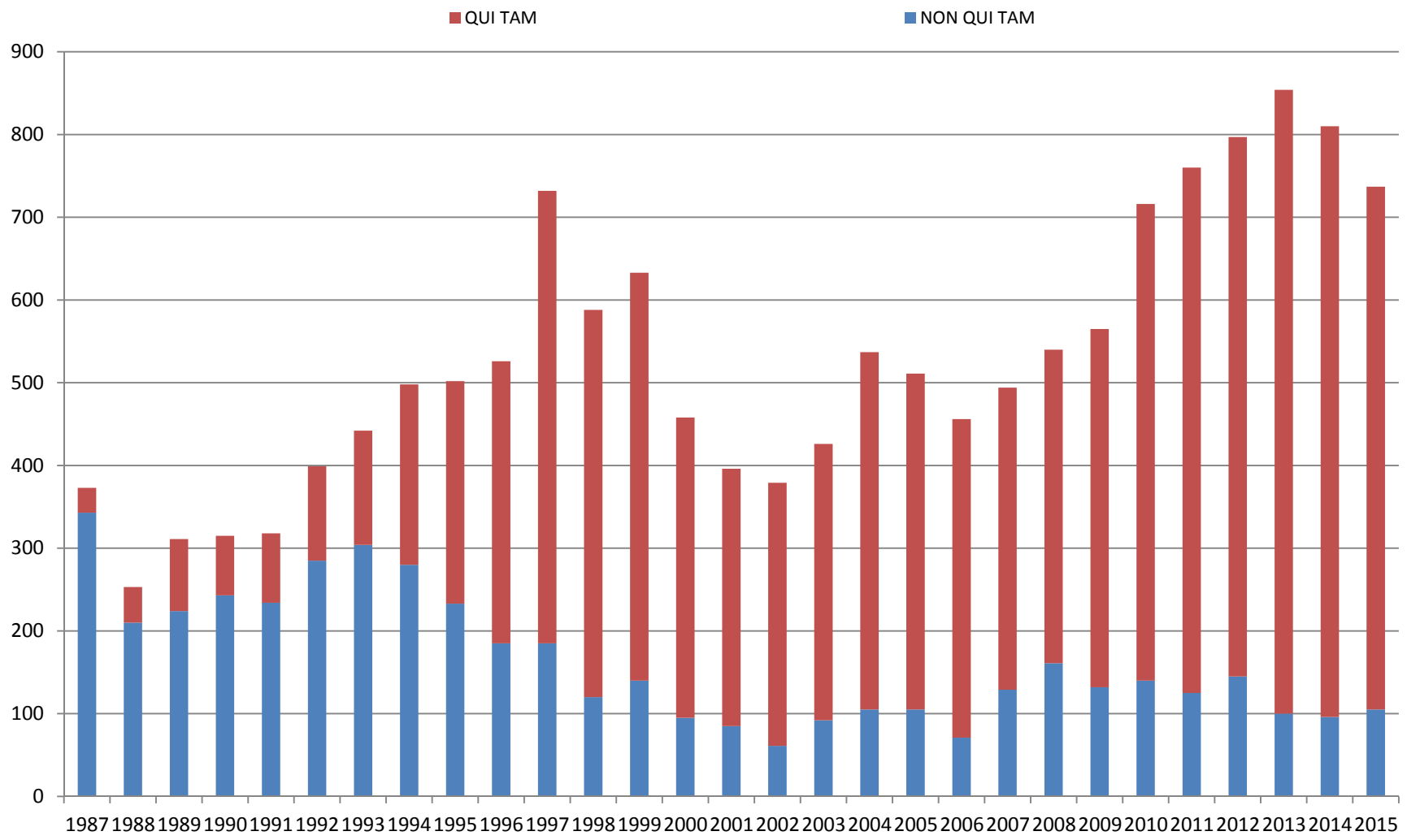


- ***Trends***
  - DOJ has continued to aggressively enforce the Anti-Kickback Statute ("AKS") and the Stark Law. In 2015, particular targets for enforcement of these statutes were hospital systems, pharmaceutical companies, and healthcare providers.
  - As with other enforcement areas, FCA prosecutions in 2016 are expected to focus more on individual defendants.
  - Whistleblowers in FCA cases were especially active last year, and were responsible for triggering many of these cases—2015 saw a greater amount of whistleblower recoveries than in all previous years combined.

Update on Substance of FCA Theories

- ***Medical Necessity***: Allegations that a provider's care lacked medical necessity continues to be the primary foundation of healthcare settlements, followed by allegations based on the AKS and Stark Law. In 2015, two medical necessity cases topped $200 million.
- ***Implied Certification Theory***: In *Universal Health Services v. Escobar*, a case with potentially significant implications for FCA jurisprudence, the Supreme Court granted certiorari to review a First Circuit case concerning the viability of the "implied certification theory" of FCA liability. The case concerns allegations that a mental health center failed to supervise patients adequately. The Court will review whether the supervision was a condition of payment and if so, whether it can serve as the basis of implied certification FCA liability.
- ***Reverse False Claims***: DOJ has started to take particular interest in "reverse false claims" cases under new provisions that allow for FCA liability based on retaining overpayments, especially in the healthcare context.

False Claims Act – Annual New Matters: 1987 to 2015



2016 Enforcement Priorities

The Health and Human Services' Office of the Inspector General ("HHS OIG") outlined several priorities in its 2016 work plan. These include:

- ***Quality of care***: HHS OIG will assess how CMS uses quality reporting data provided by hospitals and the extent and effectiveness of the agency's evaluation of this data. It is particularly important that this data be complete and accurate because it forms the basis for several agency initiatives.
- ***Replacement of implementation devices***: Another HHS OIG review will focus on payments received by hospitals for the replacement of implanted medical devices, an area where improper payments are suspected.
- ***ePHI***: HHS OIG will focus on the adequacy of the Office for Civil Rights' efforts to ensure the protection of electronic protected health information, and the efficacy of audits to determine whether healthcare providers have taken sufficient protective measures to protect the privacy of this information. This review may suggest increased attention on potential Health Insurance Portability and Accountability Act violations.

CFPB Statistics and Key Trends

"To date, the Bureau's enforcement activity has resulted in more than $11 billion in relief for over 25 million consumers. Our supervisory actions have resulted in financial institutions providing more than $248 million in redress to nearly 2 million consumers. And as of this month, we have handled over 700,000 complaints from consumers addressing all manner of financial products and services."

– Richard Cordray,

CFPB Director

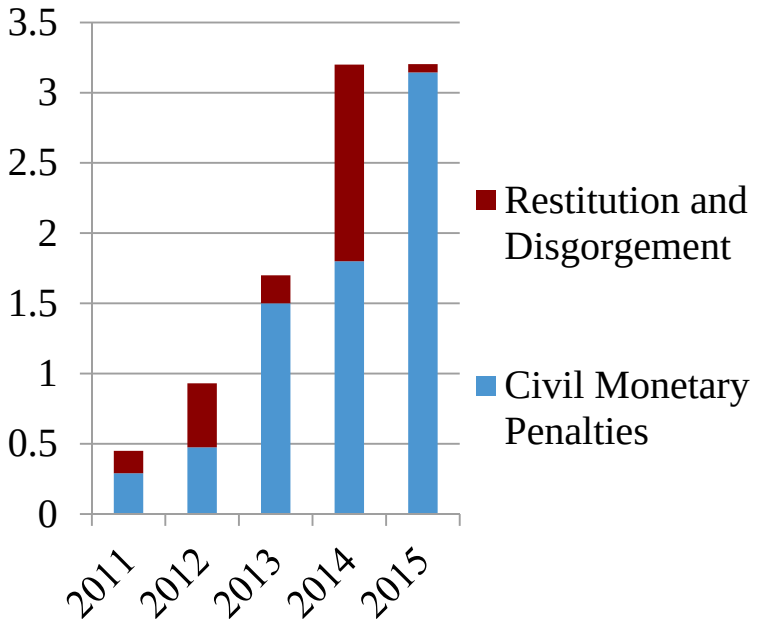
(Sept. 29, 2015)

- ***2015 Statistics***
  - The number of CFPB employees grew from 1,443 in 2014 to 1,529 in 2015 (6% increase). This represents a 231% increase from the number of CFPB employees in 2011—663 employees.
  - In 2015, the CFPB received $485 million in transfers from the Fed—an increase of 299% from 2011 ($162 million).
- ***Trends***
  - Companies should expect increased regulation of controls on banks, credit unions and mortgage companies.
  - The CFPB is focused on four main priorities in 2016 for mortgage lenders—the ability-to-repay rule, loan originator compensation plans, marketing service agreements, and the TILA-RESPA Integrated Disclosures rule.

CFTC Statistics and Key Trends

- CFTC filed 69 enforcement actions in 2015 focusing on manipulation, spoofing and fraud and ensuring that market participants meet their regulatory requirements.
- Significant actions:
  - Enforcement of the Commodity Exchange Act's (CEA) anti-spoofing clause, including its action, along with DOJ, against Navinder Sarao;
  - Use of the CEA's new anti-manipulation authority; and
  - Enforcement actions against swaps markets intermediaries to ensure their compliance with supervision and reporting obligations.
- The CFTC also continued its prosecution of benchmark rate manipulation cases, imposing the largest monetary penalty in CFTC history ($800 million) against a large foreign financial institution for manipulation of LIBOR.

CFTC Recovery (in billions)



FIRREA Update

- ***Key Trends***
  - DOJ has evinced an increased willingness to aggressively interpret and utilize FIRREA to prosecute alleged malfeasance by financial institutions. Among other reasons, the statute appeals to prosecutors because it requires a lesser standard of proof (violations must be proven by a preponderance of the evidence, as opposed to beyond a reasonable doubt) and has a longer statute of limitations (10 years, as opposed to the usual 5-year time frame of many federal criminal statutes).
- ***Notable cases***
  - In February 2015, Standard & Poor's Financial Services LLC ("S&P") settled with DOJ and nineteen states for over $1.375 billion in the largest ever settlement with a credit rating company. According to then-Attorney General Holder, S&P "engaged in a scheme to defraud investors by knowingly issuing inflated credit ratings," acting from a "desire for increased profits and market share to favor the interests of issuers over investors."
  - In June 2015, in *U.S. v. Heinz*, the Second Circuit endorsed an expansive interpretation of FIRREA, endorsing its application to frauds which "affect" a financial institution even where the bank is not the target of the fraud.

Criminal Tax Update

- Dozens of anticipated NPA resolutions have emerged from the DOJ Tax Division's August 2013 "Program for Non-Prosecution Agreements or Non-Target Letters for Swiss Banks" (the "DOJ Tax Swiss Bank Program").
  - DOJ announced the DOJ Tax Swiss Bank Program in conjunction with the Swiss Federal Department of Finance.
  - As of January 6, 2016, 76 Swiss banks had received NPAs from DOJ under the DOJ Tax Swiss Bank Program.

- DOJ has settled with some banks already under criminal investigation at the time the DOJ Tax Swiss Bank Program was announced, and is resolving its investigations of others. Julius Baer recently announced an agreement in principle with DOJ to settle its investigation for $547 million.

Virtual Currency Update

- In June 2015, NY DFS released the first regulatory framework for virtual currencies. This framework requires a "BitLicense" for firms engaged in services related to the utilization of virtual currency.
  - Requirements include maintaining specific capital requirements; protecting customer assets; submitting reports and financial statements; establishing an anti-money laundering program; and establishing a cybersecurity program, among other things.

- In September 2015, the Conference of State Bank Supervisors ("CSBS") issued a final model regulatory framework for virtual currency activities designed to assist state regulatory agencies in licensing and supervising virtual currency activities.
- In September 2015, the CFTC brought its first action against an unregistered Bitcoin options trading platform, the San Francisco-based Coinflip, Inc., and its CEO for violations of the Commodity Exchange Act and CFTC regulations.

Spotlight on the Financial Sector

- The costs of compliance for financial institutions continue to rise as regulation continues to be stringently enforced.
- A June 2015 study estimated that sixteen major banks spent over $300 billion on fines and legal bills since 2010.
- In November 2015, Moody's calculated that litigation costs incurred by banks since the 2008 financial crisis had reached almost $219 billion, and that the lion's share of these costs were borne by banks in the United States.
- The Office of the Comptroller of the Currency estimated that compliance with the Volcker Rule, which became effective on April 1, 2014, could cost financial institutions as much as $4.3 billion—primarily for larger organizations.

Federal Rules Updates

On December 1, 2015, a number of changes to the Federal Rules of Civil Procedure became effective. Key changes included the following:

- **Rule 4(m)**: Expansion of time frame to serve a complaint and summons from 90 to 120 days.
- **Rule 26(b)(1)**: Institution of requirement that discovery must be "relevant" to party claims and/or defenses and "proportional to the needs of the case."
- **Rule 26(c)(1)(B)**: Clarification that protective orders may shift the cost of discovery. However, parties should generally assume that the "responding party ordinarily bears the costs of responding"; this change should not lead parties to think that "cost-shifting should become a common practice."
- **Rule 34**: Prohibition of boilerplate objections; the rule explains that objections "must state with specificity the grounds for objection" and disclose "whether any responsive materials are being withheld."

Proxy Access Overview

- Proxy access was the pivotal governance issue of 2015 and remains a prominent topic for 2016.
- "Proxy access" means providing shareholders the ability to include one or more shareholder-nominated director candidates for election in a company's proxy statement and on the company's proxy card.
- ***Mandatory Rule.*** In 2011, courts struck down an SEC rule (Rule 14a-11) that would have required companies to provide proxy access to nominate up to 25% of the board to any group of shareholders that collectively owned 3% of a company's stock for three years.
- ***"Private Ordering."*** Proxy access may still be implemented under state law through amendments to a company's governing documents. Shareholders can submit proposals through the Rule 14a-8 shareholder proposal process for inclusion in a company's proxy statement requesting that a company take the steps necessary to provide for proxy access.
- Institutional shareholders such as BlackRock, State Street, and Vanguard, as well as proxy advisory firms such as ISS and Glass Lewis, generally support proxy access.

Proxy Access: Shareholder Proposals and Bylaw Adoptions

- For the 2015 proxy season, more than 100 U.S. public companies received a proxy access shareholder proposal, and 88 of these went to a vote. As of January 17, 2016, at least 114 companies have received proxy access shareholder proposals, including several companies that have already adopted proxy access provisions.
- Shareholder proposals typically request that any group of shareholders that collectively owned 3% of a company's stock for three years have proxy access for director candidates representing up to 25% of the board.
- As of January 17, 2016, at least 141 have adopted proxy access provisions.
- More than 100 S&P 500 companies have adopted proxy access including 32 of Fortune 100 companies and half of Dow 30 companies.

Year	Proxy Access Proposals Submitted	Voting Results*	Average Level of Support**	Total Majority Votes**
2015	114	88	55.2%	54
2014	24	18	30.9%	6
2013	21	16	33.1%	5
2012	24	12	29.0%	2

Source: Gibson, Dunn & Crutcher; ISS; and Alliance Advisors.
*Excludes proposals on ballots but not presented at, or withdrawn before, the annual meeting.
** Based on "for" votes as a percentage of "for" and "against" votes.

Dodd-Frank Act Rulemaking Update

- In August 2015, the SEC adopted final rules to implement the CEO pay ratio provisions of the Dodd-Frank Act (§ 953(b)).

- The SEC has proposed rules to implement each of the other executive compensation-related Dodd-Frank provisions.

Dodd-Frank Provision	Final Rules Anticipated	Implementation Timing
Hedging (§ 955)	Before April 2016	First proxy statement or Form 10-K after the final rules become effective
Pay for Performance (§ 953(a))	Unknown	First proxy statement or Form 10-K after the final rules become effective
Clawbacks (§ 954)	Unknown	Also requires NYSE/NASDAQ rulemaking; first applicable filing after exchange rules become effective

- The public comment periods have closed for all of the proposed rules.

Dodd-Frank Act Rulemaking Update

Final Pay Ratio Rule

- The final pay ratio rules:
  - Require public companies to disclose the annual total compensation of the "median employee" (excluding the CEO), the annual total compensation of the CEO, and the ratio of these two amounts; and
  - Require that all employees (including non-U.S., part-time, seasonal or temporary employees) of the company and its consolidated subsidiaries be included in the process of identifying the median employee.
- For most companies, the pay ratio disclosure will be required for their 2018 proxy statements with respect to fiscal year 2017 compensation.
- Commissioners Gallagher and Piwowar both dissented, and there are pending House and Senate bills seeking to repeal Section 953(b) of Dodd-Frank regarding the pay ratio rules.

Dodd-Frank Act Rulemaking Update

Proposed Executive Compensation-Related Rules

- In February 2015, the SEC proposed rules under Dodd-Frank requiring disclosure in companies' proxy statements of whether they permit any employees (including officers) or directors to engage in transactions that are designed to, or have the effect of, hedging or offsetting any decrease in the market value of company stock.
- In April 2015, the SEC proposed rules under Dodd-Frank requiring each company to disclose information showing the relationship between executive compensation "actually paid" to the CEO, and the other named executive officers (in the aggregate), and the company's financial performance.
- In July 2015, the SEC proposed rules under Dodd-Frank directing the stock exchanges to require the adoption and disclosure of clawback policies, providing:
  - If a company is required to prepare an accounting restatement due to material noncompliance with any financial reporting requirement, the company will recoup from any current or former "executive officers" any "excess incentive-based compensation" paid during a three-year look-back period; and
  - Recovery would be on a "no-fault" basis, and a company would have discretion not to seek recovery only if the direct expense of doing so would exceed the amount to be recovered.

PCAOB and Audit-Related Developments

- In July 2015, the SEC issued a concept release addressing the prospect of enhanced disclosures for audit committees. The concept release contains approximately 75 numbered paragraphs, each of which asks a series of questions on a broad range of matters involving the audit committee's work.
- Specifically, the SEC's release sets forth three main areas for potential disclosure and requests comments on questions the SEC poses related to these three areas: (1) the audit committee's oversight of the independent auditor; (2) the audit committee's process for selecting the independent auditor; and (3) the audit committee's consideration of the independent auditor's qualifications.
- In June 2015, the Public Company Accounting Oversight Board ("PCAOB") issued a concept release seeking comment on the content and possible uses of audit quality indicators ("AQIs"), measures that may provide new insights into audit quality. The concept release seeks comment on 28 potential AQIs, covering three broad categories: (1) measures dealing with the availability, competence, and focus of those performing the audit; (2) measures concerning an audit firm's tone at the top and leadership, incentives, and independence, etc.; and (3) measures relating to financial statements, internal controls, and communications between auditors and audit committees.

Delaware Law Updates

- Recent cases have focused attention on provisions aimed at more effectively managing certain types of shareholder litigation as the frequency and cost of this litigation have continued to escalate. The State of Delaware has responded to this discussion by passing certain amendments to the Delaware General Corporation Law ("DGCL"), which address the validity of these provisions.
- In June 2015, the State of Delaware enacted legislation that:
  - Allows corporations to require that "internal corporate claims" be brought in the courts of Delaware while also prohibiting the use of any other jurisdiction as the exclusive jurisdiction; and
  - Prohibits stock corporations from including fee-shifting provisions for internal corporate claims in their certificates of incorporation or bylaws.
- In December 2015, in *In re: Vaalco Energy Inc. Consolidated Shareholder Litigation*, Vice Chancellor Laster of the Delaware Chancery Court declared that any certificate or bylaw provision that purports to prohibit the removal of directors without cause is invalid under the DGCL unless the company has a classified board or cumulative voting. In the case, Vaalco filed an exhibit that purports to list 175 public companies whose articles or bylaws contain exactly that type of provision.

Other Governance Matters

- ***Board Diversity***
  - A recent report by the Government Accountability Office found that "greater gender balance [on boards] could take many years," even as the percentage of women on S&P 1500 boards rose from 8% in 1997 to 16% in 2014.
  - Rep. Carolyn Maloney plans to unveil a bill that would require public companies to report their strategies for recruiting more women to board and senior management positions.
- ***Environmental and Political Contributions/Lobbying Disclosures***
  - Environmental shareholder proposals (*e.g.*, climate change, GHG emissions) remain among the most frequently submitted shareholder proposals, averaging support of approximately 24% of votes cast when put to a vote.
  - Although the total number of political contributions/lobbying disclosure shareholder proposals decreased from 2014 to 2015, these proposals remain a frequent topic that averages support of approximately 29% of votes cast when put to a vote.
- The level of board oversight of these areas of shareholder interest continues to be a topic of debate.

1: GAO Report on Strategies to Address Representation of Women Include Federal Disclosure (Dec. 2015).

International Regulatory & Enforcement Trends

International Regulatory & Enforcement Trends

- Developments at the World Bank
- Updates by Jurisdiction
  - United Kingdom
  - European Union
  - Brazil and Latin America
  - China and Asia
- International Cooperation

Developments at MDBs

- In October 2015, Leonard McCarthy, the Integrity Vice President of The World Bank Group, reported that in 2015:
  - The Bank prevented approximately $138 million across 20 contracts from being awarded to companies that had attempted to engage in misconduct;
  - Integrity Vice Presidency investigations led to the debarment of 71 entities; and
  - The Bank's "response to fraud and corruption risks covered 61 projects and 93 contracts worth about $523 million."
- In December 2015, the African Development Bank Group announced that it had reached a settlement to impose a one-year conditional debarment on Hitachi Ltd. for the company's commission of sanctionable practices on a South African power project.
- The World Bank, which regularly makes referrals to national authorities (including sharing evidence gained in its anti-corruption investigations), recently announced that it would be limiting this practice pending the outcome of an appeal before the Supreme Court of Canada that challenges the Bank's immunity in connection with its 2011 cooperation with the Royal Canadian Mounted Police investigation into the SNC-Lavalin matter.

United Kingdom Enforcement Update

Serious Fraud Office (SFO)

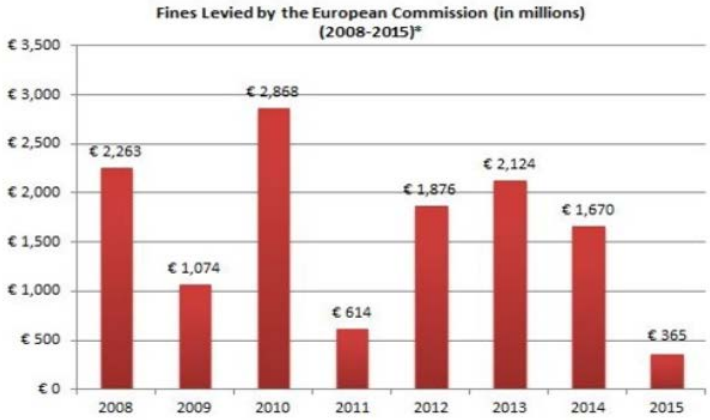
- In November 2015, the SFO announced its first public DPA hearing in connection with its investigation of a U.K. based bank. DPAs were introduced in 2014 as an official means to settle corporate investigations in the U.K. Previous attempts by the SFO to use DPAs were criticized by judges on the basis that determining penalties was properly the role of the judiciary.
- The SFO has been active in aggressively pursuing alleged wrongdoers even outside of the U.K.—as examples, the former head of the Nigerian Security, Minting and Printing Company and former Nigerian Oil Minister—in order to face charges of corruption and money-laundering.

Financial Conduct Authority

- In November 2015, the FCA instituted its largest-ever fine for financial crime failings to Barclays Bank—£72,069,400—after finding that Barclays failed to minimize the risk that it might be used to facilitate financial crime. The fine represented the bank's profit on the deal plus a £19m penalty. Although the FCA made no finding that the underlying transaction involved financial crime, it charged Barclays with failing to institute the higher levels of diligence required for the PEP clients implicated by the transaction.

European Union Update

- ***Italian Corporate Governance Code Amendment.*** In July 2015, the Italian Corporate Governance Committee amended the Corporate Governance Code of Italian Listed Companies to introduce corporate social responsibility requirements—e.g., that boards allocate authority for corporate social responsibility matters—and whistleblowing principles, including providing anonymous channels to employees to report any irregularity or breach of applicable laws or internal procedures.



In 2015, the European Commission imposed €365 million (approximately $391 million) in fines.

- ***U.S. Safe Harbour Decision.*** In October 2015, the European Court of Justice ("ECJ") overturned a 2000 decision by the European Commission that the personal data of EU residents could be transferred to the U.S. consistent with the EU Data Protection Directive through the Safe Harbour Program, which provides that the transfer of personal data to a third country is permissible only if that country ensures an adequate level of protection. The ECJ found that the U.S. "does not afford an adequate level of protection of personal data" for EU citizens, , thus invalidating the Safe Harbour Program and more generally raising questions about how to handle EU-US data transfers.

The Americas Update

Brazil

- ***Anti-Corruption.*** In September 2015, the CGU issued "Integrity Programs – Guidelines for Private Companies," establishing five pillars for Brazilian corporate compliance programs:
  - Commitment and support from senior management;
  - Adequate authority and autonomy of the compliance function;
  - The creation of a company-specific, risk-based integrity program;
  - Structuring of corporate compliance rules and instruments; and
  - Ongoing monitoring and testing of the compliance function.

- ***Anti-Competition***
  - Brazil's Competition Authority ("CADE") has pushed the boundaries of Brazilian antitrust law by pursuing charges against companies for issuing an "invitation to collude." In June 2015, for example, CADE fined Brazil's Federal Council for Auditing based on the theory that it tried to unilaterally "influence the adoption of a uniform conduct."
  - Investigations continued in "Operation Car Wash" and into foreign exchange rates.
  - CADE published preliminary versions of its Guidelines for Competition Compliance Programs and of FAQs regarding its leniency program.

The Americas Update

Canada

- ***Anti-Corruption***
  - The Canadian government remains committed to enforcing the Corruption of Foreign Public Officials Act ("CFPOA"). In February 2015, the Royal Canadian Mounted Police charged SNC-Lavalin Group Inc. with one count of fraud and one count of violating the CFPOA for allegedly paying approximately 47.7 million CAD in bribes to Libyan government officials.
  - Canada's Extractive Sector Transparency Measures Act ("ESTMA") came into effect in June 2015. The ESTMA requires covered entities to "report annually on payments made to governments relating to the commercial development of oil, natural gas, or minerals, at home and abroad."

- ***Anti-Competition***
  - In June 2015, the Canadian Competition Bureau ("CCB") issued its Corporate Compliance Programs Bulletin, which recognizes the implementation of a "credible and effective" compliance program as a mitigating factor for determining corporate fines. The CCB will treat the existence of an effective compliance program as a mitigating factor even if it fails to completely prevent improper conduct.
  - The CCB suffered a blow in late 2015 when the Public Prosecution Service of Canada decided to drop a high-profile prosecution into an alleged chocolate cartel.

The Americas Update

Mexico

- ***Anti-Corruption.*** In May 2015, President Enrique Peña Nieto signed comprehensive legislative and institutional reforms into law. These reforms, which now await implementing legislation, would have wide-ranging effects. Among other things, they would: (1) grant the Federal Audit Office the power to search government books and records at any time; (2) create a special anti-corruption prosecutor's office to handle criminal corruption investigations; and (3) impose liability on companies influencing the awarding of licenses and concessions.

- ***Anti-Competition***
  - In May and June 2015, the Mexican Federal Economic Competition Commission adopted three new guidelines regarding: (1) the initiation of investigations for anti-competitive practices; (2) the conduct of investigations for anti-competitive practices; and (3) Mexico's leniency program.
  - A new Federal Economic Competition Law approved by the Mexican Congress became effective in 2014, but has yet to be tested.

Asia Anti-Corruption Update

- ***China***
  - Three years into President Xi Jinping's anti-corruption campaign, domestic corruption prosecutions show no signs of abating, and if anything have expanded into legislative reforms, high-profile arrests, and international outreach.
  - Business executives and government officials alike should be alert to the outsized risk of whistleblower reports, with four out of five anti-corruption investigations by Chinese authorities reportedly being initiated by whistleblowers.
- ***India.*** In August 2015, police in Goa arrested Satyakam Mohanty, the former vice president of Louis Berger International Inc., for his alleged role in the conduct at issue in the company's above-described settlement with DOJ.
- ***Korea.*** Corruption scandals continue to engulf the political landscape in Korea; in August 2015, President Park Geun-Hye announced criminal pardons of over 6,000 individuals and several leaders of *chaebol* companies have been found guilty of corruption-related offenses in recent years only to be pardoned or released on parole.

Asia Anti-Competition Update

Asian anti-competition regulation has followed the lead of the U.S., Europe, and Brazil. Significant developments include the following:

- In May 2015, the Japanese Fair Trade Commission ("JFTC") expanded its extraterritorial jurisdiction by ruling for the first time that the Japanese Antimonopoly Act can apply to a cartel whose conduct occurred outside of Japan, where the conduct had the effect of substantially restraining competition in Japan.
- In September 2015, the Korean Fair Trade Commission signed a memorandum of understanding ("MOU") with the DOJ and U.S. Federal Trade Commission to pledge ongoing cooperation in international enforcement matters. Korea joins China, India, and Japan, all of which have MOUs with the U.S.
- In September 2015, Singapore proposed new procedures for its leniency guidelines which would require applicants to unconditionally admit to the conduct for which they seek leniency and to allow the Competition Commission of Singapore permission to contact other jurisdictions aware of the conduct.
- In December 2015, Hong Kong's new Competition Ordinance took effect to prohibit bid rigging, market allocation, and price fixing regardless of where it occurs so long as it harms competition in the jurisdiction.

International Cooperation

In 2015, U.S. enforcement authorities prioritized cross-border anti-corruption prosecutions in cooperation with their foreign counterparts. For example:

- U.K. and Nigerian anti-corruption enforcement agencies have been cooperating since 2013 to investigate suspected bribery and money laundering in the Nigerian energy sector.
- In late September 2015, during Chinese President Xi Jinping's visit to Washington, D.C., President Obama agreed that the U.S. government would recognize and enforce property confiscation judgments rendered by Chinese courts in anti-corruption cases. The two presidents promised to expand law enforcement and anti-corruption cooperation, including by enhancing coordination and cooperation on criminal investigations, repatriation of fugitives, and asset recovery issues.
- The SFO's November 2015 civil action against a U.K. based bank was part of a coordinated global settlement with the SEC; the bank was charged with violations of both the U.K. Bribery Act and the FCPA. The SEC required the bank to disgorge $8.4 million, but deemed that this was satisfied by the bank's payment of an equal amount to U.K. authorities.

Building & Overseeing Effective Compliance

Building & Overseeing Effective Compliance

- The Path Forward: Practical Recommendations for Navigating Through the Uncertainty:
  - Addressing Cyber Risk
  - Being Prepared for the New Activism
  - Building Global Compliance
  - Mitigating Individual Liability
  - Managing Regulatory Change
- The Common Themes of Compliance

Addressing Cyber Risk

- ***Integrate Technology Expertise at the Board and Senior Management Levels.***[1] Consider including a technology expert on your board or as a member of senior management who can advise on (1) erecting safeguards against the possibility of cyber attack and (2) maintaining an effective overall technology approach at a company-wide level.
  - A February 2015 survey found that 80% of boards do not receive advice on their company's cyber security strategy.[2]
  - Cyber-expertise should ideally be one of the criteria the board assesses when evaluating candidates for board and senior management positions.
- ***Clarify Oversight.*** Clearly identify where responsibility for cyber-matters ultimately sits (*e.g.*, risk committee versus audit committee) and chain-of-command/communication protocols.
- ***Simulate Breach.*** Consider engaging third-party expertise to assess the company's protocols and protections, identify weaknesses, and assist in creating a plan of action should breach occur.

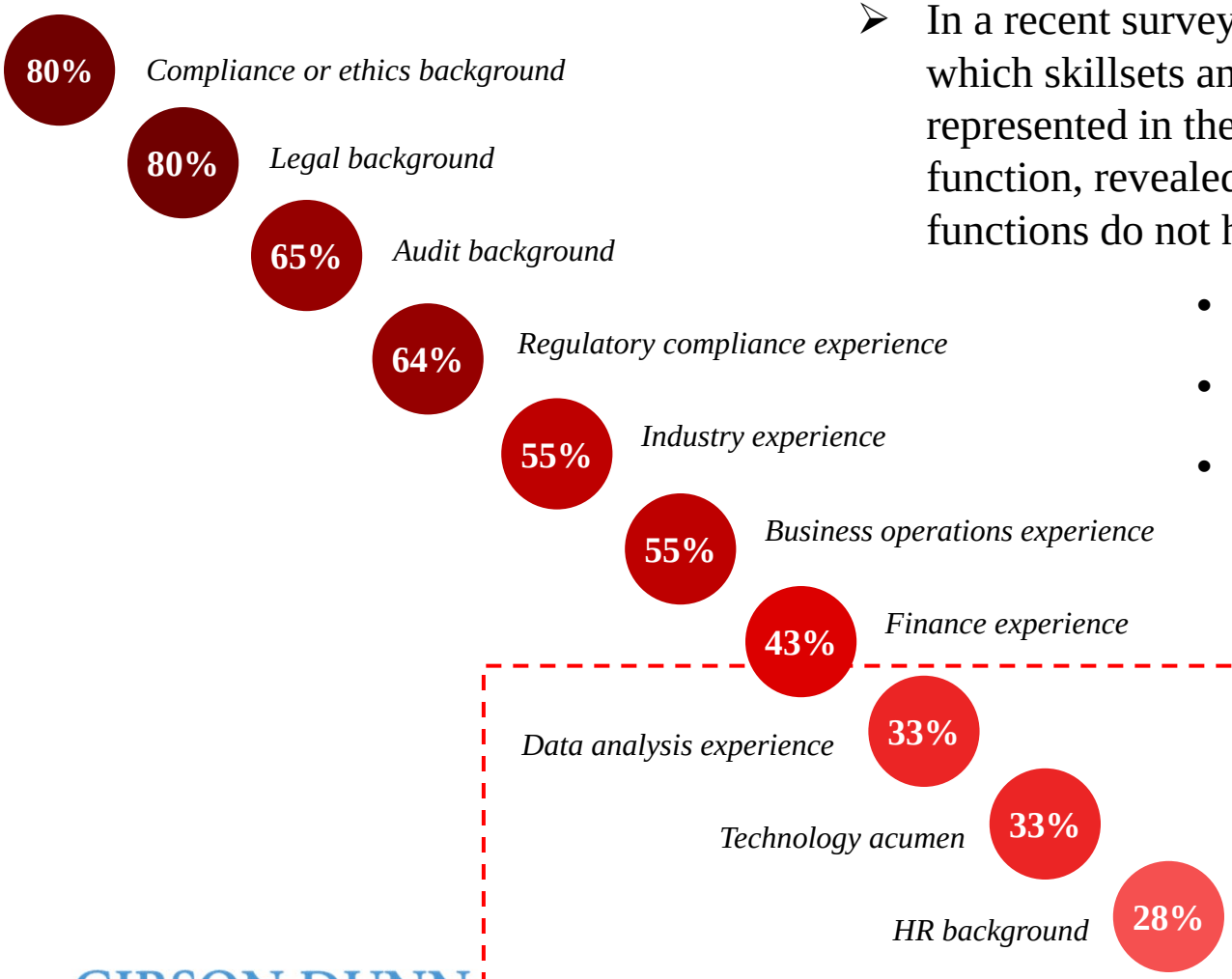
1: HBR
2: http://www.raytheon.com/news/rtnwcm/groups/gallery/documents/content/rtn_233811.pdf

Addressing Cyber Risk

- ***Consider an Inter-Department Approach***. The rising incidence and cost of security breaches have shown that siloed management of cybersecurity no longer works. Effective management of cybersecurity risks requires collaboration among teams with technology acumen, legal knowledge, compliance expertise, risk management experience, and business understanding.
  - Information technology and legal departments, the compliance function, business managers, and external stakeholders should all work together effectively to protect the business.[1]
- ***Provide Effective Cybersecurity Training to Employees***. Companies should regularly train employees at all levels on how to maintain effective safeguards against the risk of cyberattack—and the magnitude of possible ramifications should these protections fail. Consider offering training to third parties such as vendors and business partners for additional coverage.
- ***Track Evolving Guidance***. As standards change, so should your company's approach to cybersecurity, and existing policies should be updated to reflect best practices. Maintaining compliance with regulatory expectations—for example, from NY DFS, the FCC, the FTC, and the SEC—will not only guard against possible later charges of deficiency, but will help to ensure that protections are effective.

1:2015 PWC State of Compliance Survey

Addressing Cyber Risk



- In a recent survey,[1] respondents, when asked which skillsets and experience were represented in their companies' compliance function, revealed that many compliance functions do not have significant:
  - Data analysis experience;
  - Technology acumen; and
  - HR experience.

- Companies seeking to mitigate cyber risk should consider building data and technology expertise in the compliance function.

GIBSON DUNN

1: 2015 PWC State of Compliance Survey.

Being Prepared for the New Activism

Analyze existing shareholder base

- Monitor shareholder activity.
- Investor relations should identify, log, monitor and brief the internal working group on all communications.

Maintain a dialogue with shareholders

- Maintain lines of communication (key shareholders should not hear from the company for the first time only after an activist has become involved).
- Use effective messaging to define financial and strategic goals.
- Understand potential motivations for support of activists.

Review bylaws and corporate governance policies

- While most activists focus on performance issues, they will often exploit structural vulnerabilities.

Source: Activist Insight

Being Prepared for the New Activism

Identify and coordinate your response team	➢ Create a standing response team. ➢ Engage a financial adviser and law firm to assess the company through the eyes of an activist/unsolicited bidder.
Consider strategy regarding rights plan	➢ Consider creating an "on the shelf" rights plan strategy.
Brief board on shareholder engagement developments	➢ Directors should be kept up-to-date on all dealings with activists/bidders and institutional shareholders.
Prepare possible responses by company to identified vulnerabilities	➢ Traditional takeover defenses are no longer as effective.

Source: Activist Insight

Building Global Compliance

Tip 1: Keep Compliance Hand-in-Hand With Strategy

- Compliance professionals can offer valuable insights into the strategic planning process, yet, according to a recent survey, while 78% of CEOs are concerned about overregulation and its impact on their ability to achieve the company's goals, only 35% of CCOs are involved in strategic planning.
- Beyond improving a company's ability to manage global enforcement trends, compliance that works hand-in-hand with strategy can be a part of how a company distinguishes itself in the marketplace.

"I have found that you can predict a lot about the likelihood of an enforcement action by asking a few simple questions about the role of the company's compliance department in the firm: Are compliance personnel included in critical meetings? Are their views typically sought and followed? Do compliance officers report to the CEO and have significant visibility with the board? Is the compliance department viewed as an important partner in the business and not simply as a support function or a cost center? Is compliance given the personnel and resources necessary to fully cover the entity's needs?"

- Andrew Ceresney, Director, SEC Division of Enforcement (Nov. 4. 2015)

1: 2015 PWC State of Compliance Survey.

Building Global Compliance

Tip 1: Keep Compliance Hand-in-Hand With Strategy

- For companies seeking to grow into new industries or geographical regions, involving the compliance function in strategy discussions may be particularly helpful.
- Keeping compliance at the table during strategic negotiations can also help enforce the view of compliance as a critical partner rather than the "watchdog."
- Introducing compliance to strategic partners early on, particularly with partners in jurisdictions other than the U.S., can help create relationships that foster a culture of compliance.

56% of CEO respondents globally say their companies are likely to compete in new industries over the next three years.

– 2015 PWC State of Compliance Survey

Building Global Compliance

Tip 2: Assess Your Culture

- Cultural assessment should be part of the company's risk assessment process.
- In a recent survey,[1] cultural assessment ranked dead last among the responsibilities CCOs have. If the CCO has an incomplete understanding of the company's true culture, practical program elements, such as training regarding the code of conduct and whistleblower retaliation, may be less effective.

"For me, the risk assessment is at the center of the effort to manage compliance risk . . . . If you have a robust enterprise-wide risk assessment process, your priorities will evolve out of that . . . . [T]he effectiveness of your compliance program is really based on the maturity and quality of the risk assessment process."

- Director at Deloitte Financial Advisory Services LLP

While building a "culture of compliance" is frequently touted as a critical aspect of effective compliance, it can be challenging to identify practical to-dos.

1: Deloitte ,2015 Compliance Trends.

Building Global Compliance

Tip 3: Manage the Scope of Expanding Compliance

- The responsibilities of compliance professionals continue to expand, and managing the expanding scope of the compliance function is more challenging than ever.
- Despite this expanding scope, it remains important to consolidate oversight of the compliance function, in order to enable the CCO to provide the CEO and Board with a direct "line of sight" into all key compliance responsibilities.
- Managing the expanding scope of compliance while maintaining consolidated oversight requires developing a clear understanding of responsibilities and where obligations sit in the company. To this end, consider:
  - Developing a "who-to-go-to-when" responsibilities map;
  - Maintaining action plans for key compliance events; and
  - Identifying compliance-related issues as "ownership," "monitoring," or "line of sight" issues.

Building Global Compliance

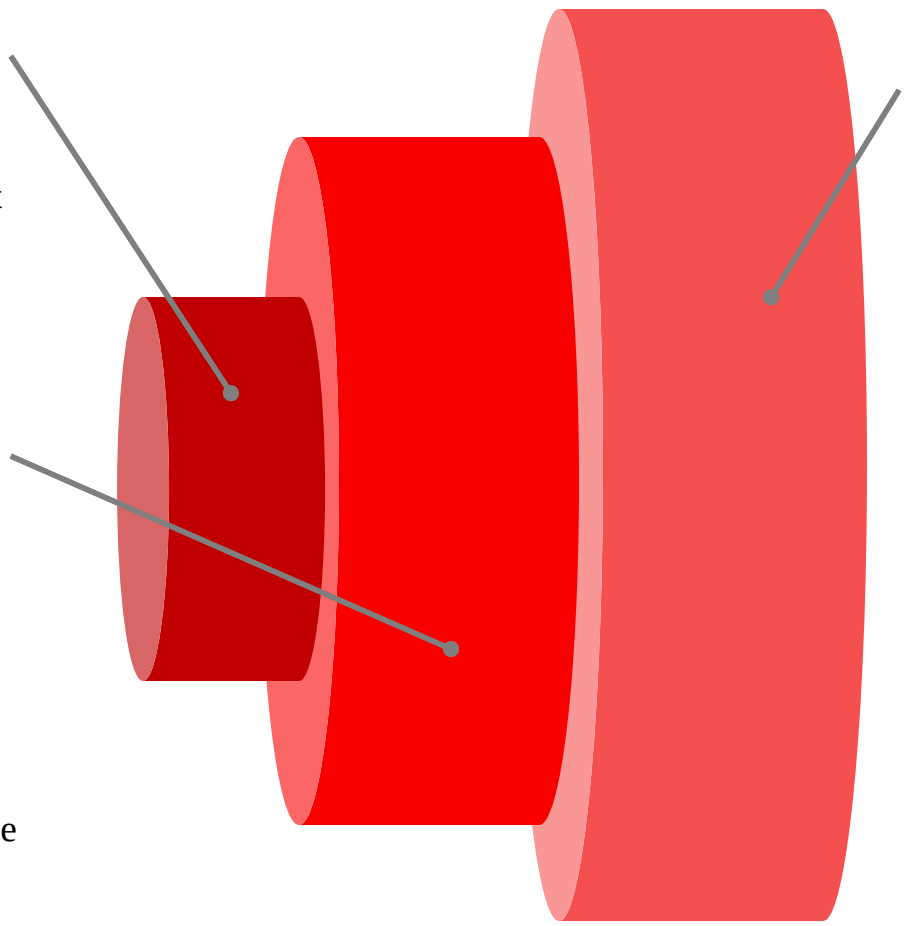
Tip 3: Manage the Scope of Expanding Compliance (Example Only)[1]

Ownership

- Code of conduct
- Anti-bribery
- Corporate policy management
- Data privacy
- Conflicts of interest

Monitoring

- Government contracting
- Product claims
- Workplace Safety / OSHA
- Insider trading
- Social media and technology
- Competition
- Product safety and compliance
- Third-party due diligence
- Customs and trade compliance



Line of Sight

- Product labeling
- M&A diligence / integration
- Records management
- Conflict minerals
- IP / Confidentiality
- Contracts and strategic agreements
- Business continuity
- Labor and employment

GIBSON DUNN

1: This graph is from the 2015 PWC State of Compliance Survey.

Building Global Compliance

Tip 3: Manage the Scope of Expanding Compliance; How Many Hats?

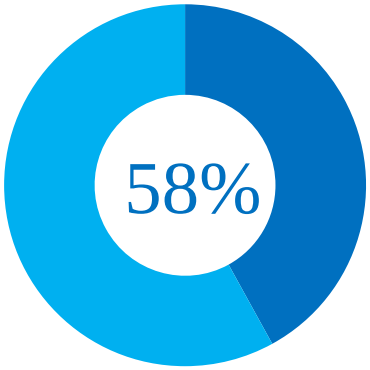
- In part because of the expanding scope of compliance, it is important that compliance professionals remain free of conflicts of interest and, while integrated into the business, focused on the tasks of compliance.

"The vast majority of these cases involved CCOs who 'wore more than one hat,' and many of their activities went outside the traditional work of CCOs, such as CCOs that were also founders, sole owners, chief executive officers, chief financial officers, general counsels, chief investment officers, company presidents, partners, directors, majority owners, minority owners, and portfolio managers."

- Luis A. Aguilar, SEC Commissioner (June 29, 2015)

Building Global Compliance

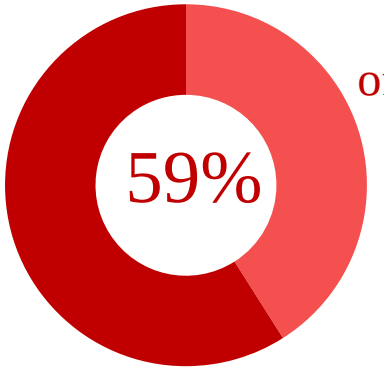
Tip 4: Close the IT Gap



of CCOs are confident or very confident that the right metrics are being used to gauge compliance program effectiveness.[1]

- In a recent survey,[1] only 32% of compliance professionals responding were confident or very confident in their IT systems, and most indicated that they primarily use desktop software or internally developed tools for most compliance tasks.

- While big data and GRC tools have a lot of potential, the rapid evolution of technology, coupled with the fact that many compliance executives do not have extensive IT experience, means that much of this potential goes untapped.



of CCOs are only somewhat confident or not confident at all that the IT systems the compliance department uses can fulfill the department's reporting and responsibility tasks.[1]

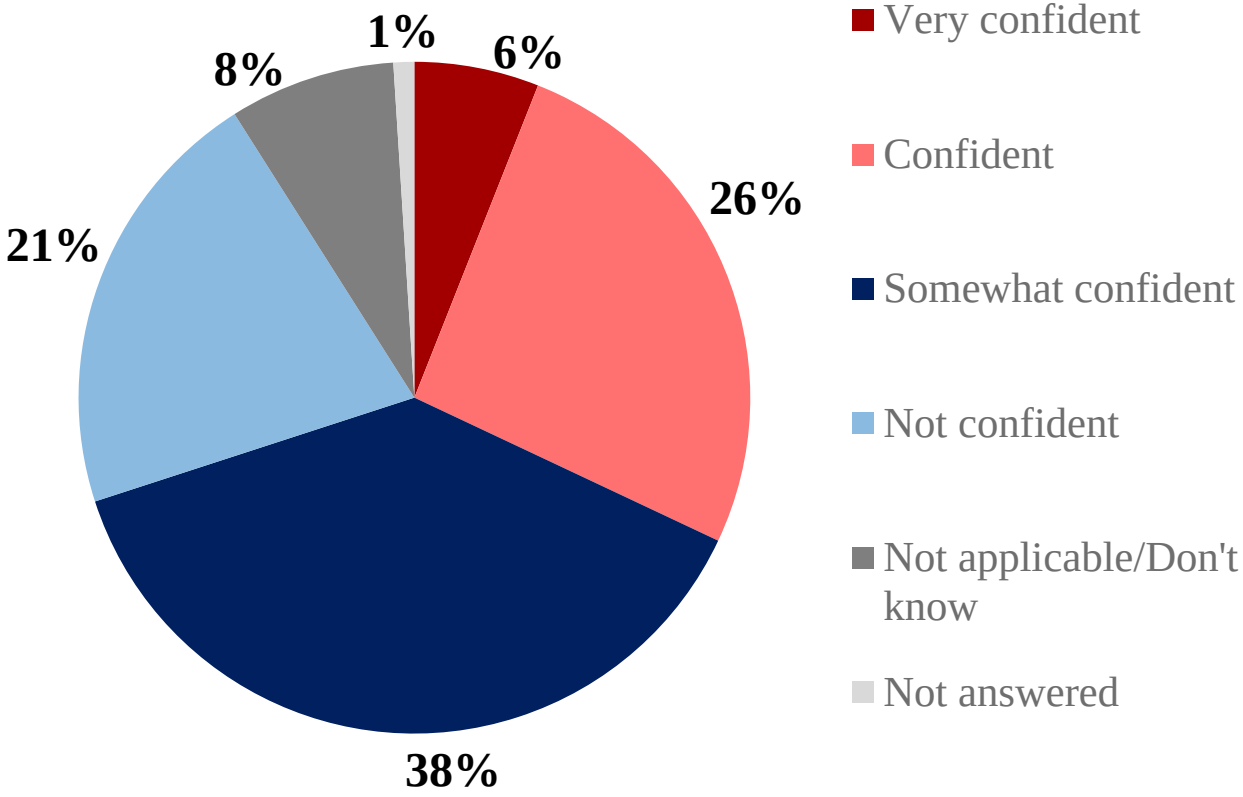
1: 2015 Deloitte Compliance Trends

Building Global Compliance

Tip 4: Close the IT Gap

- Finding the right technology for your compliance function can help the company identify and utilize the right metrics for assessing compliance.
- Objective metrics identified and implemented through the right technology can help make the business case that leadership can expect to see a return on their investment if the compliance budget is increased.

How confident are you in the ability of your compliance department's IT systems to fulfill your organization's compliance responsibilities and reporting requirements?



GIBSON DUNN

1: 2015 Deloitte Compliance Trends

Mitigating Individual Liability

- The specter of personal liability can be mitigated by observing certain best practices, including:
  - Regular evaluation of risks posed by organizational weaknesses, and utilization of external counsel to advise related decision-making;
  - Taking responsibility for and ensuring timely remediation of identified issues;
  - Staying abreast of current developments and industry trends to ensure that job performance conforms to standards and regulatory expectations;
  - According proper weight to "red flags" and other signals of possible deficiencies or illegal activity; and
  - Escalating problems up reporting lines to senior personnel to ensure that the organization is fully aware of all material issues and potential issues.

Managing Regulatory Change

- Thomson Reuters' recent Annual Cost of Compliance Survey found that 70% of respondents expected an increase in the amount of regulatory information published during the next year.
- Companies should implement systems to track regulatory changes in real time, evaluate their impact on the company's operations, and make the necessary changes to conform with new regulations.

  - The use of automated systems may help identify the relevant regulatory changes, while minimizing the risk of error.
  - Companies should clearly allocate responsibility for responding to regulatory changes within the compliance function.

The Common Themes of Compliance

- A common baseline of globally accepted Anti-Bribery Compliance Program ("ABC") Principles can be distilled from prevailing global best practices, including:
  - ***The laws and regulations of leading nations in anti-corruption, including***: the United States, China, and the United Kingdom, among others; and
  - ***Non-governmental regulations and guidelines, including***: the UN Global Compact; OECD Good Practice Guidance on Internal Controls and related guidelines, Ethics, and Compliance; World Bank Group Integrity Compliance Guidelines; ISO Standards 19600, 31000, and draft ISO 37001; and ICC Rules on Combating Corruption, among others.
- Analysis of these and other best practices yields common themes in ten key areas:

- Policy and Control Framework
- Compliance Function
- Compliance Risk Assessment and Compliance Program Evaluation
- Case Handling
- Compliance Messaging
- Internal & External Assurance Providers
- Third Party Risks
- Supplier Contracting Controls and Procurement
- Finance Controllership Function
- Mergers & Acquisitions

Today's Panelists

F. Joseph Warin

1050 Connecticut Avenue, N.W.
Washington, D.C. 20036-5306, USA
Tel: +1 202.887.3609
FWarin@gibsondunn.com

F. Joseph Warin is chair of the Washington, D.C. Office's Litigation Department, which consists of over 125 attorneys. Mr. Warin also serves as co-chair of the firm's White Collar Defense and Investigations Practice Group. He served as Assistant United States Attorney in Washington, D.C. from 1976-83. In that capacity, Mr. Warin was awarded a Special Achievement award by the Attorney General. As a prosecutor, he tried more than 50 jury trials. Mr. Warin acted as Independent Monitor for Statoil and Alliance One, and was appointed U.S. Counsel to the German Monitor for Siemens.

Mr. Warin's areas of expertise include white collar crime and securities enforcement – including Foreign Corrupt Practices Act investigations, False Claims Act cases, special committee representations, compliance counseling and complex class action civil litigation. Mr. Warin has handled cases in more than 35 states. His clients have included corporations, officers, directors and professionals in regulatory, investigative and trial matters. These representations have involved federal regulatory inquiries, criminal investigations and Congressional hearings. Recently, Mr. Warin successfully argued motions to dismiss in securities and consumer protection class actions in the Southern District of New York and the District of Columbia.

For many years, Mr. Warin has been hired by audit committees or special committees of public companies to conduct investigations into allegations of wrongdoing. These investigations have been in a wide variety of industries including energy, oil services, health care, and telecommunications.

Mr. Warin has conducted FCPA investigations relating to business in 35 countries, including, Argentina, Austria, Bangladesh, Brazil, China, Croatia, Dubai/UAE, France, Germany, Great Britain, India, Iran, Iraq, Italy, Jordan, Kazakhstan, Korea, Lebanon, Libya, Mexico, Nigeria, Norway, Panama, Peru, Philippines, Poland, Qatar, Russia, Saudi Arabia, South Africa, and Yemen. In connection with these investigations, Mr. Warin has provided advice to general counsels and senior management regarding company practices, enhancements to compliance programs, disciplinary action for company employees and remedial measures for improving compliance. Some investigations have also prompted voluntary disclosures to the SEC and DOJ, and Mr. Warin handled the DOJ and SEC investigations.

Mr. Warin has been listed in *The Best Lawyers in America* every year from 2006 to 2015 for White Collar Criminal Defense. *Benchmark Litigation* named him a U.S. White Collar Crime Litigator Star and a Local Litigator Star in Washington, D.C. for White Collar Crime in both 2013 and 2014. Mr. Warin graduated from the Georgetown University Law Center, where he was Editor of Law and Policy in International Business. He received his Bachelor of Arts degree *cum laude* from Creighton University, where he was student body president. After graduation he served as a law clerk for United States District Court Judge J. Calvitt Clarke, in the Eastern District of Virginia. Mr. Warin has been a member of the American Bar Association's White Collar Criminal Law Committee since 1988 and served as president of the Assistant United States Attorneys Association.

He is a member of the Board of Directors of the Washington Lawyers Committee for Civil Rights.

Scott D. Hammond

1050 Connecticut Avenue, N.W.
Washington, DC 20036-5306, USA
Tel: +1 202.887.3684
SHammond@gibsondunn.com

Scott D. Hammond is a partner in the Washington, D.C. office of Gibson, Dunn & Crutcher and co-chair of the firm's Antitrust and Competition Practice Group. Before joining Gibson Dunn, Mr. Hammond served as a U.S. Department of Justice prosecutor for 25 years. Most recently, he served for eight years as the Antitrust Division's Deputy Assistant Attorney General for Criminal Enforcement – the highest ranking career lawyer in the Antitrust Division. In that capacity, he was responsible for supervising all of the Department of Justice's domestic and international criminal antitrust investigations as well as overseeing all of the criminal antitrust litigation nationwide. Mr. Hammond oversaw the work of more than 100 federal prosecutors and led criminal prosecutions in a wide range of industries, including auto parts, LIBOR, municipal bonds, LCD panels, air transportation, real estate foreclosure auctions, construction, chemicals and coastal freight. He personally tried criminal antitrust cases and has directed the litigation of dozens of jury trials. In addition, he assisted in overseeing all of the Antitrust Division's criminal appellate work between 2005 and 2013.

Mr. Hammond assists clients in antitrust and white-collar crime compliance, crisis management and government investigations across all industry sectors. Mr. Hammond provides clients with know-how on the Department of Justice's latest strategies for monitoring and uncovering antitrust and related federal violations which can also be employed by companies to design effective compliance programs as well as to ensure early detection of violations. Timely detection can result in a complete pass from prosecution for companies and their executives under the Antitrust Division's Corporate Leniency Program that Mr. Hammond helped implement and that he oversaw while at the Division. In addition, Mr. Hammond was instrumental in the design and implementation of similar leniency programs in dozens of jurisdictions around the world.

Mr. Hammond's practice focuses on the representation of clients in cross border investigations running in parallel with U.S. Department of Justice investigations. During his tenure at the Antitrust Division, he was the principal point of contact for cartel matters with senior competition officials abroad and oversaw the Department's coordination of joint investigations with numerous jurisdictions, including the European Union, Australia, Brazil, Canada, Chile, Germany, Japan, Korea, Mexico, The Netherlands, New Zealand, Singapore, South Africa, Switzerland, and the United Kingdom. As a result, Mr. Hammond is well-versed in the anti-cartel enforcement investigative powers as well as the policies and practices of every major competition enforcement authority. His experience allows clients to create a comprehensive and integrated global strategy to assess and mitigate their potential exposure to criminal, civil and administrative sanctions by enforcement agencies working in tandem across the globe.

Mr. Hammond was recently selected by his peers for inclusion in *The Best Lawyers in America*© 2016 in the field of Antitrust Law and was also named a 2016 "Litigation Star" by *Benchmark Litigation*: *The Definitive Guide to America's Leading Litigation Firms and Attorneys*.

Alexander H. Southwell

200 Park Avenue
New York, NY 10166-0193, USA
Tel: +1 212.351.3981
ASouthwell@gibsondunn.com

Alexander H. Southwell is a partner in Gibson, Dunn & Crutcher's New York office and is Co-Chair of Gibson Dunn's Privacy, Cybersecurity, and Consumer Protection Practice Group. His practice focuses on counseling a variety of clients on privacy, information technology, data breach, theft of trade secrets and intellectual property, computer fraud, national security, and network and data security issues, including handling investigations, enforcement defense, and litigation. In particular, Mr. Southwell regularly advises companies victimized by cyber-crimes and counsels on issues under the Computer Fraud and Abuse Act, the Economic Espionage Act, the Electronic Communications Privacy Act, and related federal and state statutes. Mr. Southwell additionally handles a range of white-collar criminal and regulatory enforcement defense, internal investigation, compliance, and complex civil litigation matters. An experienced trial and appellate attorney, prior to joining Gibson Dunn, Mr. Southwell served as an Assistant United States Attorney in the United States Attorney's Office for the Southern District of New York.

Mr. Southwell is also an Adjunct Professor of Law at Fordham University School of Law where he teaches a seminar on cyber-crimes, covering computer misuse crimes, intellectual property offenses, the Fourth Amendment in cyber-space, computer evidence at trial, data breach and privacy issues, and information security, among other areas.

Mr. Southwell earned his undergraduate degree, *magna cum laude*, from Princeton University and his Juris Doctor, *magna cum laude*, from New York University School of Law. Following law school, Mr. Southwell was a Law Clerk for the Honorable Naomi Reice Buchwald of the United States District Court for the Southern District of New York.

Mr. Southwell is also a member of Gibson Dunn's Electronic Discovery and Information Law, Intellectual Property, White Collar Defense and Investigations, Crisis Management, Litigation, and Appellate and Constitutional Law Practice Groups. Mr. Southwell also serves on Gibson Dunn's Firmwide Diversity Committee and is active with the Federal Bar Council and the Association of the Bar of the City of New York, having previously served on the Committee on Information Technology Law, Professional Responsibility Committee and the Government Ethics Committee. In addition, Mr. Southwell serves on the Board of Advisors of the Center on Law and Information Policy at Fordham Law School, one of the nation's leading academic centers contributing to the development of the law and policy in the area of information technology, and served on the Advisory Board of the Cybersecurity Law Institute at Georgetown University Law Center. Mr. Southwell is also a member of the New York Chapter of InfraGard, a partnership between the FBI and the private sector dedicated to sharing information and intelligence to prevent hostile acts against the United States' cyber and physical infrastructure.

Lori I. Zyskowski

200 Park Avenue
New York, NY 10166-0193, USA
Tel: +1 212.351.2309
LZyskowski@gibsondunn.com

Lori Zyskowski is a partner in Gibson Dunn's New York office. She is a member of the Securities Regulation and Corporate Governance Practice Groups. Ms. Zyskowski has extensive experience as a corporate securities and governance lawyer, with a focus on SEC compliance and disclosure issues, corporate governance best practices, state corporate laws, the Sarbanes-Oxley Act of 2002, the Dodd-Frank Act of 2010 and SEC regulations.

Prior to joining Gibson Dunn, she was an in-house corporate lawyer at General Electric. In her most recent role as Executive Counsel, Corporate, Securities & Finance, Ms. Zyskowski advised GE's board of directors and senior management on corporate governance and securities law issues. She was responsible for outreach to institutional investors on governance and executive compensation issues and overseeing the company's review and response to shareholder proposals. She oversaw the company's periodic reporting, registered offerings, proxy statement and other SEC and NYSE filings. Ms. Zyskowski also advised on mergers, acquisitions, dispositions and financial services regulatory matters.

Before that, Ms. Zyskowski was Corporate and Securities Counsel and Assistant Secretary at Pitney Bowes from 2006 to 2009. In that capacity, she served as the Secretary of the Audit Committee and Counsel to the Executive Compensation Committee of Pitney Bowes' board of directors. She was responsible for managing the securities governance department, which oversaw director and officer ownership reporting and subsidiary management.

From 2002 to 2005, she served as the Assistant General Counsel, Securities, at MeadWestvaco. Following the adoption of the Sarbanes-Oxley Act, she was responsible for designing and implementing the new corporate governance processes under the NYSE corporate governance listing standards for MeadWestvaco.

Ms. Zyskowski is a frequent speaker on governance, proxy and securities disclosure panels and is very active in the corporate governance community. She is a member of the board of directors of the Society of Corporate Secretaries and Governance Professionals and served as Secretary to the board from 2011 to 2013.

She graduated from Columbia University School of Law in 1996 and was a Harlan Fiske Stone Scholar.

Adam M. Smith

1050 Connecticut Avenue, N.W.
Washington, DC 20036-5306, USA
Tel: 202.887.3547
ASmith@gibsondunn.com

Adam M. Smith is of counsel in the Washington, D.C. office of Gibson, Dunn & Crutcher. He is an experienced international lawyer with a focus on international trade compliance and white collar investigations, including with respect to federal and state economic sanctions enforcement, the Foreign Corrupt Practices Act, embargoes, and export controls.

From 2010-2015 Mr. Smith served in the Obama Administration as the Senior Advisor to the Director of the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) and as the Director for Multilateral Affairs on the National Security Council. At OFAC he played a primary role in all aspects of the agency's work, including briefing Congressional and private sector leadership on sanctions matters, shaping new Executive Orders, regulations, and policy guidance for both strengthening sanctions (Russia and Syria) and easing measures (Burma and Cuba), and advising on enforcement actions following sanctions violations.

Mr. Smith travelled extensively in Europe, the Middle East, Asia, Africa, and the Americas conducting outreach with governments and private sector actors on sanctions, risk, and compliance. This outreach included meetings with senior leadership in several sectors including finance, logistics, insurance and reinsurance, energy, mining, technology, and private equity.

Mr. Smith frequently chaired the Treasury delegation to EU/G7 consultations regarding Russia sanctions and negotiated with EU institutions and member states to implement coordinated measures. Additionally, Mr. Smith managed the development and implementation of the U.S. government's international outreach program on Congressionally-mandated Iran sanctions and helped develop proposed sanctions-relief strategies as a part of the Iranian nuclear negotiations.

During Mr. Smith's tenure on the White House's National Security Council he advised the President on his multilateral agenda including with respect to international sanctions, coordinated inter-agency efforts to relieve U.S. economic restrictions on Burma, and developed strategies to counter corruption and illicit flows and to promote stolen asset recovery.

Sarah E. Fortt

1050 Connecticut Avenue, N.W.
Washington, D.C. 20036-5306, USA
Tel: 202.887.3501
SFortt@gibsondunn.com

Sarah Fortt is an associate in the Washington, D.C. office of Gibson, Dunn & Crutcher, practicing in the Securities Regulation and Corporate Governance and Executive Compensation and Employee Benefits Practice groups. Ms. Fortt has advised clients, including public companies and their boards of directors, on a wide array of matters, including corporate governance best practices, executive compensation-related matters, Securities and Exchange Commission reporting and exchange requirements and issues and shareholder proposal matters. Ms. Fortt also advises non-profit organizations on corporate governance issues.

Ms. Fortt received her J.D. from Yale Law School in 2010 and graduated *summa cum laude* from Gordon College in 2004. Prior to joining Gibson Dunn, Ms. Fortt practiced in the executive compensation and benefits department at Cravath, Swaine & Moore LLP.

Ms. Fortt is admitted to practice in the State of New York and the District of Columbia.

Our Offices

Beijing
Unit 1301, Tower 1
China Central Place
No. 81 Jianguo Road
Chaoyang District
Beijing 100025, P.R.C.
+86 10 6502 8500

Brussels
Avenue Louise 480
1050 Brussels
Belgium
+32 (0)2 554 70 00

Century City
2029 Century Park East
Los Angeles, CA 90067-3026
+1 310.552.8500

Dallas
2100 McKinney Avenue
Suite 1100
Dallas, TX 75201-6912
+1 214.698.3100

Denver
1801 California Street
Suite 4200
Denver, CO 80202-2642
+1 303.298.5700

Dubai
Building 5, Level 4
Dubai International Finance Centre
P.O. Box 506654
Dubai, United Arab Emirates
+971 (0)4 370 0311

Hong Kong
32/F Gloucester Tower, The Landmark
15 Queen's Road Central
Hong Kong
+852 2214 3700

London
Telephone House
2-4 Temple Avenue
London EC4Y 0HB
England
+44 (0)20 7071 4000

Los Angeles
333 South Grand Avenue
Los Angeles, CA 90071-3197
+1 213.229.7000

Munich
Hofgarten Palais
Marstallstrasse 11
80539 Munich
Germany
+49 89 189 33-0

New York
200 Park Avenue
New York, NY 10166-0193
+1 212.351.4000

Orange County
3161 Michelson Drive
Irvine, CA 92612-4412
+1 949.451.3800

Palo Alto
1881 Page Mill Road
Palo Alto, CA 94304-1125
+1 650.849.5300

Paris
166, rue du faubourg Saint
Honoré
75008 Paris
France
+33 (0)1 56 43 13 00

San Francisco
555 Mission Street
San Francisco, CA 94105-0921
+1 415.393.8200

São Paulo
Rua Funchal, 418, 35° andar
Sao Paulo 04551-060
Brazil
+55 (11)3521.7160

Singapore
One Raffles Quay
Level #37-01, North Tower
Singapore 048583
+65.6507.3600

Washington, D.C.
1050 Connecticut Avenue, N. W.
Washington, D.C. 20036-5306
+1 202.955.8500