Challenges In Compliance And Corporate Governance

Eleventh Annual Webcast

F. Joseph Warin
Richard Grime
Scott Hammond
Lori Zyskowski

January 27, 2015

GIBSON DUNN

MCLE Certificate Information

- **MCLE Credit 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 1.5 credit hours, of which 1.5 credit hours may be applied toward the areas of professional practice requirement. This course is NOT approved for 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 1.5 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 1.5 hours. Regulated by the Solicitors Regulation Authority (Number 324652).
- Application for approval is pending with the Texas, Virginia, and Washington State Bars.
- Attorneys viewing the webcast as a group will need to sign a CLE attendance sheet. Prior to the start of the webcast, please contact Jeanine McKeown (National Training Administrator) at 213-229-7140 or jmckeown@gibsondunn.com to request the CLE attendance sheet.
- Most participants should anticipate receiving their certificates of attendance via e-mail in approximately 3 to 4 weeks following the webcast.

Presentation Overview

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

Building & Overseeing Effective Compliance

Building & Overseeing Effective Compliance

- Key Compliance Challenges for the Good Governance Company
- Evolving Areas of Risk
- Update on Enterprise-Wide Compliance Matters
- Updates on Other Current Governance Topics

The Good Governance Company

The key challenges companies now face are how to:

- Measure and prove the compliance program's effectiveness;
- Make compliance concepts accessible across every level of the organization;
- Link compliance programs to other aspects of corporate responsibility; and
- Connect the dots with risk assessment, training, and audit functions.

A "good governance" company will evolve its compliance program to address these challenges.

Measuring and Proving the Effectiveness of Compliance

- Federal Sentencing Guidelines require companies to evaluate the effectiveness of their compliance programs.
- Though many companies measure effectiveness, not all are confident in their approach:
  - A recent survey[1] indicates that 71% of midsize to large companies regularly assess the effectiveness of their programs.
  - Effectiveness is cited as a top concern of compliance professionals,[2] and another recent survey[3] of midsize to large companies indicates that only about ½ of compliance professionals have a high degree of confidence in the metrics they use.
  - The metrics used most often focus on measuring activities (e.g., hotline call analysis, training completion rates), rather than impact.

"You realize that there are certain things where you cannot be measured on a scale of 1 to 10. Integrity, for example. You cannot be six on a scale of 1 to 10. That's not integrity. Business integrity is either 10 or zero, and nothing in between."

– Lamberto Andreotti, CEO
Bristol-Myers Squibb

- **Examples:**
  - A global biopharmaceutical company regularly surveys employees to assess effectiveness.
  - A multinational food and beverage company uses both internal and third-party evaluations of its compliance program.

1: PricewaterhouseCoopers LLC State of Compliance Survey (2014). Survey respondents included more than 1,000 large companies.
2: NAVEX Global Ethics and Compliance Training Benchmark Report (July 2014).
3: Deloitte, Compliance Week, Compliance Trends Survey (2014); 209 respondents with annual revenues of $1 to $5 billion.

Measuring and Proving the Effectiveness of Compliance

Metrics That Measure Impact Versus Activity

Commonly-Used Compliance Program Effectiveness Metrics		
Program Effectiveness Metrics[1]	**2014**	**2013**
Compliance audit results	66%	71%
Risk assessment results	61%	65%
Training completion rates	53%	**
Hotline/helpline metrics	50%	56%
Results from regulatory visit	48%	46%
Customer & other third party feedback/complaints	39%	41%
Employee questionnaires or culture surveys	35%	52%
Employee disclosures (e.g., conflicts of interest, gifts)	35%	56%
External benchmarking	33%	**
Internal benchmarking	28%	**
Training competency tests	24%	**
Cost of non-compliance (e.g., penalties, litigation)	22%	44%
Exit interview responses	20%	**
Cost of compliance program activities	19%	17%
Training trend analysis	17%	**
Monitoring of press and public statements	16%	24%
Aging and disposition of litigation and enforcement	14%	20%

Many of the most commonly-used metrics only measure the level of compliance-related activities.

Of equal or greater value are metrics that measure the level of impact the compliance program has on the business.

GIBSON DUNN

1: PricewaterhouseCoopers LLC State of Compliance Survey (2014).

Making Compliance Concepts Accessible Across the Organization

"3 Key Questions To Ask Whenever You Are Unsure:

1. ***How would this decision look to others?***
2. ***Am I willing to be held accountable for this decision?***
3. ***Is this consistent with GE's Code of Conduct?"***

– GE's Simple Reference Guide

- Encouraging greater participation and engagement at each level of the organization remains challenging for many companies and a priority among compliance professionals.[1]
- Creating cultures of compliance remains challenging, particularly in foreign jurisdictions.
- Because compliance is behavior-driven, consistency and frequency of message is critical.

- **Examples:**
  - GE's Code of Conduct and global integrity policies are summarized into four simple principles:[2] (1) be honest, fair, and trustworthy, (2) obey applicable laws and regulations, (3) fulfill your obligation to be the "voice of integrity" and promptly report any concerns, and (4) work to run the company with speed, accountability, and compliance. The company also provides employees with a two-page simple reference guide.
  - An international avionics and information technology company has an interactive mobile app from which employees can seek compliance guidance for various situations.

1: Deloitte, "Compliance Survey 2014: The Changing Role of Compliance Officers."
2: GE, "The Spirit & The Letter," Statement of Integrity (2014).

Connecting Compliance to Other Aspects of Corporate Responsibility

- Many companies are now viewing compliance as only one prong of corporate responsibility, and are seeking to link compliance to corporate community outreach, sustainability, and diversity and inclusion efforts.
- Investors groups are interested in how these other areas of corporate responsibility influence risk and profitability, and are putting pressure on companies and regulators to address these issues more thoroughly.
- **Examples:**
  - An international computer software, electronics, and hardware company produces an annual "Citizenship Report" related to corporate responsibility, and profiles its compliance efforts alongside its community outreach, human rights, and environmental sustainability activities. Both corporate citizenship and compliance matters are overseen by the board through its regulatory and public policy committee.
  - A U.S.-based toy manufacturer's "Global Citizenship Report" includes evaluations of the company's compliance performance alongside its performance in corporate responsibility areas, including environmental sustainability.

Connecting the Dots on Risk Assessments, Training, and Audits

- Many companies do not link the results of their risk assessments to their training programs and audits. Using a targeted, risk-based approach can help companies identify gaps and allocate resources.
- According to a recent survey, training accounts for the largest percentage of most compliance program budgets,[1] and is the single most important factor in creating ethical cultures. Yet, companies may struggle to show a clear connection between training and audit results.
  - Recently, the SEC's Andrew Ceresney stressed the importance of a robust risk assessment and discussed the importance of having more than a "paper" program.
  - **Example:**
    - An international manufacturer has a global legal and regulatory risk assessment that it runs in parallel to the risk assessment performed by its "Risk Center of Excellence." The two risk assessments inform the annual compliance training strategies.
    - A global investment banking, securities, and investment management firm produces a risk report that identifies its top risks and how the company is monitoring and addressing them.

1: NAVEX Global Research, 2014 Key Trends for Ethics and Compliance Planning.

Taking a Risk-Based Approach to Audits

- As the breadth of areas requiring compliance oversight grows, so too does the need for more focused approaches to compliance.
- An enterprise-wide process of defining and prioritizing policies, standards, and controls can assist large, international companies in identifying key compliance vulnerabilities and gaps.

"As you know, there is no off-the-rack, one-size-fits-all compliance program. Companies must tailor compliance programs to manage their unique risks."

– Marshall L. Miller, DOJ Deputy Assistant Attorney General (Oct. 7, 2014)

- Risk assessments should take place across business segments (e.g., C suite, legal, finance, business units) and locations, and be integrated into the business.
- A recent survey[1] by the Ethics Resource Center found that the greatest risks exist overseas at the local level. Budget and headcount should be directed toward locations that present the highest level of risk.
- **Example:**
  - Chevron first developed a risk-based approach to compliance in 2001, and has updated its approach to account for new regulation since then, enabling its compliance function to "turn on a dime."[2]

1: Ethics Resource Center, National Business Ethics Survey of the U.S. Workforce (2014).
2: Operational Excellence Management System, Chevron, (2010); Case Study: A Risk-Based Audit At Chevron, Compliance Week (June 27, 2006).

Industry Focus on Financial Services

- Following increased regulatory attention in the wake of the financial crisis and high-profile scandals affecting the financial services industry, a robust compliance function appears to have become the new standard.
  - A recent survey[1] of compliance professionals from 222 financial institutions reveals that:
    - 93% have a dedicated compliance position, 73% of which are single-function;
    - The compliance function predominantly reports to the chief legal officer, the CEO, the chief risk officer, or the board (or board committee); and
    - Compliance with industry-specific regulations remains a primary focus.
- A recent poll on how companies are perceived by the U.S. public indicates that positive ratings of financial services companies – which traditionally score low on reputation– grew significantly.[2] Improvement in the reputation of large financial institutions was particularly noted.

1: PriceWaterhouseCoopers "State of Compliance 2014 Financial Services Industry Brief."
2: The Harris Poll 2013 RQ – February 2013.

Key Challenges: Compliance Takeaways

- Consider including metrics that measure compliance program impact in addition to or instead of metrics that only measure the level of compliance-related activities. Metrics that can measure impact include internal and external assessments and surveys and benchmarking.[1]
- Require director on-site visits each year to help inform directors, establish a record of good governance, fulfill *Caremark* duties, and strengthen the compliance culture.
- An annual compliance update to the board of directors that includes members of management across business segments can help directors identify key areas of risk and better oversee enterprise-wide compliance.
- Take a "marketing" approach to keeping employees tuned in to potential compliance issues. Key catch phrases are more likely to be remembered in moments of stress.
- Studies suggest that employees may take more seriously behaviors that will be considered in their evaluations. Consider rewarding employees who report concerns that lead to improvements.
- Consider offering trainings that speak directly to the key risks identified in risk assessments and measuring employees' post-training awareness.

1: PricewaterhouseCoopers LLC State of Compliance Survey (2014).

Evolving Areas of Risk

- Cyber-Security and Technology-Based Risks
- Reputational Risks
- Third-Party Risks

Cyber-Security: Risk Trends and Challenges

- In the past few years, cyber-attacks have become more sophisticated, and greater connectivity among corporate systems has made many companies more vulnerable.
- A recent study found that employees and subcontractors (whether disgruntled or merely poorly trained) are the greatest source of security incidents, and that this internal threat rises each year.[1]

Some estimates predict that
$9 - $21 trillion
of global economic value creation could be at risk if companies and governments are unsuccessful in combatting cyber threats.

One recent study[1] found that
80% of the total value of the Fortune 500 now consists of intellectual property and other intangibles.

- In 2014, the SEC held a roundtable on cybersecurity, during which participants discussed board involvement, disclosure, and risk management, and the SEC's Office of Compliance Inspections and Examinations released a risk alert on its initiative to assess cybersecurity preparedness in the securities industry.

1: The Global State of Information Security Survey 2015 - PriceWaterhouseCoopers National Association of Corporate Directors (NACD), Cybersecurity: Boardroom Implications (2014).

Cyber-Security: Recent Developments

- In December 2014, a multinational financial services company discovered that one of its own financial advisers had downloaded account data for approximately 350,000 of its wealth-management clients. Information on approximately 900 of these clients was later posted online.
- The November 2014 hack of a multinational technology and media company crippled the company's network and led to the theft and publication of corporate and personal information, the destruction of company servers, and the deletion of valuable internal data.
- In July 2014, a U.S.-based bank was compromised by hackers, who stole the personal information of approximately 76 million individuals.
- An online retail company announced in March 2014 that the credentials of over 176 million users had been compromised.
- During the 2013-2014 holiday season, a U.S. retail company suffered a data breach that resulted in 40 million credit and debit card numbers and 70 million personal records being stolen, a 46% drop in the company's stock price, approximately $150 million in data-breach expenses, and the resignation of the company's CEO. Several other U.S. companies have had data breaches caused, allegedly, by the same groups behind the holiday season breach.
- From 2008 to 2013, a sophisticated hacking organization penetrated the computer networks of more than a dozen major U.S. and international companies, stealing at least 160 million credit and debit card numbers, resulting in losses of hundreds of millions of dollars.
- FBI Director James Comey recently stated that it would be impossible to count how much Chinese hackers are costing the U.S. economy, but that the cost is likely in the billions.

Cyber-Security: Recent Executive Remarks[1]

- President Obama has called cyber threats one of the most serious economic and national security challenges we face as a nation, and has stated that defending against this threat would need to be a shared government-industry mission. New initiatives include:
  - New cybersecurity legislation to promote greater information sharing between the public and private sectors;
  - Increasing the ability to prosecute cyber-related crimes; and
  - A White House summit on cybersecurity and consumer protection to take place in February.
- President Obama stated nine out of ten Americans "feel like they've lost control of their personal information." He has described several new steps to counter the threat of data theft, including:
  - BuySecure initiative to encourage stronger chip-and-pin technology for credit cards;
  - Introduction of new legislation to create a single national standard on alerting possible victims of identity theft;
  - Encouragement of companies to provide customers free access to credit scores; and
  - Revitalizing the "Consumer Privacy Bill of Rights" and proposing a "Student Digital Privacy Act."
- Analysts have questioned whether the measures described by President Obama will be effective in targeting the perpetrators.

1: January 12, 2015 Remarks at the Federal Trade Commission; January 13, 2015 Remarks at the National Cybersecurity Communications Integration Center; President Obama's 2015 State of the Union Address.

Cyber-Security: Real Liabilities

- ***Reputational Damage.*** Experts estimate that the breach suffered by a multinational technology and media company will cost the company as much as $100 million, plus an unquantifiable reputational hit.
- ***Government Investigations.*** Companies that experience a cyber attack are likely to find themselves the focus of a government (e.g., FTC, attorneys general) investigation pursuant to consumer protection and other laws.

> ***"In the wake of data breaches among U.S. retailers, many believe the risk of legal liability and costly lawsuits will escalate. Today, claims by businesses that they are unaware of cybercrime risks … have become increasingly unconvincing."***
>
> **– PwC, U.S. Cybercrime Survey (2014)**

- ***10b-5 Lawsuits.*** Although securities laws have been slow to address cybersecurity issues, companies that do not address cyber-risks and experience a breach or attack are at risk of being party to subsequent suits.
- ***Shareholder Derivative Suits.*** The U.S. retail company that suffered the 2013-2014 holiday attack has been hit with several shareholder derivative suits claiming that the company failed to take the necessary steps to prevent the attack.
- ***Third Parties with Compromised Data.*** Any other individuals or entities impacted by a cyber attack at a company also may have claims against the company.

Cyber-Security: Compliance Takeaways

- ***Consider How to Provide Oversight***. The NACD Blue Ribbon Commission on Risk Governance recommends that risk oversight be a function of the full board; however, a large percentage of companies do assign risk, including cyber-risk, oversight to the audit committee or other board committee.
- ***Identify "Mission Critical" Cyber-Assets***. Complete cybersecurity is an unrealistic goal. The board and senior management should know what the company's most critical cyber-assets are, how they are accessed, and who has permission to access them.
- ***Focus on Protecting Information***. Protecting sensitive information should be considered in addition to, and independently of, preserving the integrity of networks and systems. Recent breaches have shown that information may be compromised even when networks and systems function properly.
- ***Update Your Response Plan***. Companies should ensure that they have robust, up-to-date incident response plans that have been tested.

Cyber-Security: Compliance Takeaways

- ***Take an Enterprise-wide Approach***. Consider appointing a cross-organization cyber-risk management team. All substantial stakeholder departments should be present, including business unit leaders, legal, internal audit and compliance, finance, human resources, IT, and risk management.
- ***Consider Your Third Parties***. Risk assessments should include vendors and business partners to the extent possible.
- ***Update Your Disclosure***. A company that fails to disclose cyber-related threats and then suffers even a modest attack may subsequently have to deal with lengthy and costly private lawsuits alleging inadequate public disclosure. A strong disclosure may defend against a possible securities class action by putting a reasonable investor on notice of the risk of a cyber invasion.
  - **For example**, "*We are heavily reliant on our technological infrastructure, which is one of the core foundational attributes of the company. We have attempted to safeguard that infrastructure, and periodically upgrade and adopt substantial measures to protect against invasion; however, if a breach were to occur, such breach would likely have material consequences to our business.*"[1]

1: The above is a model disclosure only and should not be utilized to protect against possible liability. Please consult legal counsel to adapt this to your own business needs.

Bitcoin Update

- Bitcoin is the most prominent form of virtual currency. Its current market capitalization is $2.5 billion, and approximately 13.7 million of a possible 21 million coins have been "mined."
- The CFTC also has oversight over swaps, futures, and options relating to Bitcoin and other virtual currencies.
- The SEC's attention to virtual currencies – which the agency has indicated would likely come under its purview – is growing.
  - In February 2014, the SEC announced a 2-week suspension of trading for Imogo Mobile Technologies—a company developing a mobile platform for Bitcoin—"because of questions that have been raised about the accuracy and adequacy of publicly disseminated information concerning, among other things, [the company's] business, revenue, and assets."
  - In June 2014, the SEC fined Bitcoin entrepreneur Erick Voorhees in connection with two offerings of unregistered securities valued in Bitcoin.
- In actions against an alleged Bitcoin Ponzi scheme, the SEC claimed that the Bitcoin investments at issue qualified as "investment contracts" and "securities." The court also determined that "bitcoin can be used as money" and that investment of Bitcoin by investors "provided an investment of money" and, thus, the interests sold were held to be securities.

Email After Hours

Managing Constant Availability

- Increasing concern over the work-related stress imposed by emails sent to employees after the business day has ended – and employees' perceived need to respond to those emails in real time – has led some companies to explore placing limits on the expectation of constant availability.
- German Labor Minister Andrea Nahles has called for an "anti-stress regulation" that would ban employers from contacting employees after the close of business. German Chancellor Angela Merkel has criticized the enactment of such an anti-stress law.[1] German law already contains strong protections for employees on vacation.
- In France, an agreement entered into within the framework of the national collective bargaining agreement[2] provides that technical and engineering consultants having a large degree of autonomy in their work (e.g., employees with management duties) who are not subject to a maximum number of working hours per day and week shall disconnect from their distance communication tools for a period of at least 11 consecutive hours each day, and at least 35 consecutive hours each week. Employers must ensure that employees have this option.
- Volkswagen has been capping its after-work email for the past three years. Specifically, the company's email servers stop routing emails to employees' work devices 30 minutes after their shifts end, and start again 30 minutes before their return to work.[2]

1: "German Government May Say 'Nein' To After Work Emails," NPR (Dec. 1, 2014)
2: Known as the "Syntec" collective bargaining agreement, amended in 2014.
3: "Volkswagen turns off Blackberry email after work hours," BBC (Dec. 23, 2011); "Banning E-mail After Work" Deutsche Welle (February 20, 2014)

Reputational Risks

- A recent Harvard Business School (HBS) study[1] finds that environmental, social, and governance (ESG) performance have become increasingly important dimensions of a company's reputation, and poor ESG practices may make companies a target for activists, harming their reputations as well as their bottom lines.
- Reputational risk is made challenging by the fact that it is:
  - Linked to risks of other kinds (e.g., product failure);
  - Shaped outside of the organization;
  - Not solely dependent on a company's own practices, but also on its supply chains.
- Reputational risks may not be easily identifiable through the quantitative assessments many companies use to identify and measure risk; thus, it is difficult if not impossible for many companies to immunize themselves against reputational risk.

In a recent survey conduced by Forbes Insights on behalf of Deloitte,[2] 88% of more than 300 directors and executives stated that they are focusing on reputational risk as a key business challenge.

1: Harvard Business School, "Monitoring the Monitors: How Social Factors Influence Supply Chain Auditors," Jodi L. Short, Michael W. Toffel, and Andrea R. Hugill (2013).
2: Deloitte, 2014 Global Survey on Reputation Risk (October 2014).

Reputational Risks: Recent Developments

Over the past few months, there have been several examples of companies dealing with reputational issues arising from:

- Executive behavior (a global technology and industrial company);
- Product failure (an international auto manufacturer);
- Workplace practices (a multinational retail company); and
- Alleged misrepresentations (a multinational banking and financial services company).

Industry Focus on Retail:[1] Global retailers came under intense reputational scrutiny following the Rana Plaza building collapse, as the spotlight of media, consumer, and investor inquiry turned to examine retailers' outsourcing practices. Many of these companies were under such intense reputational pressure that they agreed to adopt a legally binding accord requiring them to spend hundreds of millions of dollars to fund fire-safety and structural improvements in the factories of their Bangladeshi suppliers. This reveals a key challenge of reputational risk:

A company's reputation may be influenced by its own decisions, by the decisions of its suppliers, or by the decisions of other companies in its industry.

1: Harvard Business School, "Monitoring the Monitors: How Social Factors Influence Supply Chain Auditors," Jodi L. Short, Michael W. Toffel, and Andrea R. Hugill (2013).

Third-Party Risks

- ***Reputation and Third-Party Risks***. A recent HBS study[1] indicates that largely because of the risk of negative reputational spillovers, supply chain conditions are frequently cited as a top investor concern, and consumers and investors are increasingly holding companies accountable for the poor practices of their suppliers.
- ***Vendor and Supplier Risks***. A Japanese airbag maker is being investigated regarding allegations that the company hid information about a defect in its airbags that has caused automakers to recall millions of vehicles. The situation underscores the importance of in depth due diligence of suppliers. Even where a company itself has not committed any wrongdoing, it may experience severe consequences due to supplier actions.

"The best companies have adopted strong programs that include compliance personnel, extensive policies and procedures, training, vendor reviews, due diligence on third-party agents, expense controls, escalation of red flags, and internal audits to review compliance."

– Andrew Ceresney, Director, SEC Division of Enforcement, Nov. 19, 2014

1: Harvard Business School, "Monitoring the Monitors: How Social Factors Influence Supply Chain Auditors," Jodi L. Short, Michael W. Toffel, and Andrea R. Hugill (2013).

Update on Enterprise-Wide Compliance Matters

- The Board and the C-Suite
  - Compliance Committees
  - Leadership Structures
  - Succession Planning
  - Executive Compensation
- Compliance Professionals and the Compliance Department
- Senior and Middle Managers
- Whistleblowers and Employees

Compliance Committees, Certifications, and Staffing

- In a recent survey of over 1,000 large companies,[1] 36% of respondents indicated that they have no formal compliance committee. Among those companies that do, only 31% indicated that the committees include personnel from the business units.
- Approximately 8% of non-prosecution agreements (NPAs) and deferred prosecution agreements (DPAs) require changes to existing board committee structures, often requiring the creation of board compliance committees.[2] Examples include:
  - A global pharmaceutical company's DPA with the DOJ required the company to establish a board compliance committee and appoint a Chief Compliance Officer.
  - The establishment of a board compliance committee is frequently an element of settlement arrangements for healthcare companies.
- Settlements increasingly are including certification requirements. For example, the first DOJ FCPA corporate settlement agreement to require the company's CEO and CFO to "certify to [DOJ] that the Company has met its disclosure obligations" occurred in November 2014.
- A recent DPA involving an Israeli bank included the appointment of new corporate compliance and risk personnel, including a global head of cross-border activity, and empowered the Chief Risk Officer with compliance responsibilities.

1: PricewaterhouseCoopers LLC State of Compliance Survey (2014).
2: The Effect of Deferred and Non-Prosecution Agreements on Corporate Governance, Wulf A. Kaal and Timothy Lacine (2014).

A Discussion Regarding the Compliance Implications of Leadership Structures

- CEO/chairman trends indicate that,[1] although struggling companies can benefit from splitting the CEO and chairman roles, successful companies can be damaged by the same action.
- According to a study released by Korn Ferry and NACD in 2014, among S&P 500 companies, as of the end of 2012 56% had a CEO/chairman, 20% had a former executive chairman, and 23% had a non-executive chairman.
- The U.K.'s Corporate Governance Code provides that "the chairman should on appointment meet the independence criteria" set forth in the Code. Boards that decide to have a combined CEO/chairman are encouraged to consult major shareholders in advance and provide an explanation in their annual report.
- The EU's Commission Recommendation 2005/162/EC states that a significant proportion of directors should be free of any material conflict of interest.
- ***Discussion Points***. What are the compliance implications of the decision to combine the chairman and CEO roles? Can an independent board compliance committee help offset any of the perceived disadvantages of a combined CEO/chairman? What are the implications for the Chief Compliance Officer's reporting structure?

1: The Jamie Dimon Witch Hunt, Jeffrey A. Sonnenfeld, (New York Times, May 8, 2013); Splitting Top Posts Doesn't Always Work Magic, Joann S. Lublin (The Wall Street Journal, May 8, 2013).

A Discussion Regarding the Compliance Implications of Succession Planning

- Even if succession planning is assigned to a board committee, the entire board should evaluate whether board and C-suite candidates have experience addressing the company's key risks.
- Skill sets should include experience with a variety of complex compliance issues and should align with the broader corporate strategy.
- For board succession planning, consider whether to conduct an assessment of the compliance of other companies with which nominees are affiliated.
- ***Key Questions:***
  - Is, and if so, how is, a company with detailed succession plans less exposed to compliance risks?
  - How important is it to assess potential leaders based on the company's compliance culture?
  - To what extent should companies consider compliance-related experience when assessing board and C-suite candidates?
  - How should companies assess whether a candidate possesses the skills to instruct integrity and create the "tone from the top?"

McDonald's, called the "classic case study in continuity,"[1] was able to act quickly after tragedy struck because the board talked about succession at every meeting.

1: "How McDonald's Got CEO Succession Right," Patricia Sellers, Fortune (August 23, 2011).

A Discussion Regarding the Compliance Implications of Executive Compensation

- ***The Debate:***
  - "I have always been against including integrity as a [performance metric] because you cannot measure integrity on a scale from one to five … Integrity is an expectation for all employees at all times." – Lamberto Andreotti, CEO, Bristol-Myers Squibb
  - "The protocols we put in place will show we are taking the lead in demonstrating the importance of accountability in our enhanced compliance program." – Spokesman of one of the world's leading retailers, discussing the company's 2014 annual cash incentive program.
  - Other examples of companies that tie executive compensation to compliance objectives include: Colgate Palmolive, Huntsman Corp., Schlumberger Ltd., Vanguard Health Systems.
- ***Key Considerations:***
  - Should companies include compliance factors as metrics in incentive-based compensation? If so, what aspects of compliance should be included?
  - Is there a risk that companies with no or a limited ability to recoup compensation if compliance issues occur may be viewed as passing the cost of noncompliance on to shareholders?

1: Deloitte, Compliance Week, Compliance Trends Survey (2014). Percentage of question respondents listed above.

A Discussion Regarding the Compliance Implications of Clawbacks

- Although the concept of recoupment is not new, the past decade has brought a sharp rise in the number of stand-alone clawback policies, which frequently target the performance-based pay of key executives and members of management.

- Regulatory enforcement has been restricted by the confines of the Sarbanes-Oxley Act of 2002. On its face, Section 954 of the Dodd-Frank Act potentially promises more robust regulation, mandating rules requiring companies to adopt policies that provide for the recoupment of any excess incentive-based compensation received by any current or former executive officer during the three-year period preceding the date on which the company is required to issue an accounting restatement due to material noncompliance with financial reporting requirements.

- A study of large companies' policies published in April indicated that more than 70 of the 100 companies in the survey will have to amend their clawback policies in order to comply with the Dodd-Frank requirements.[1] The SEC has not yet proposed a rule to satisfy Section 954.

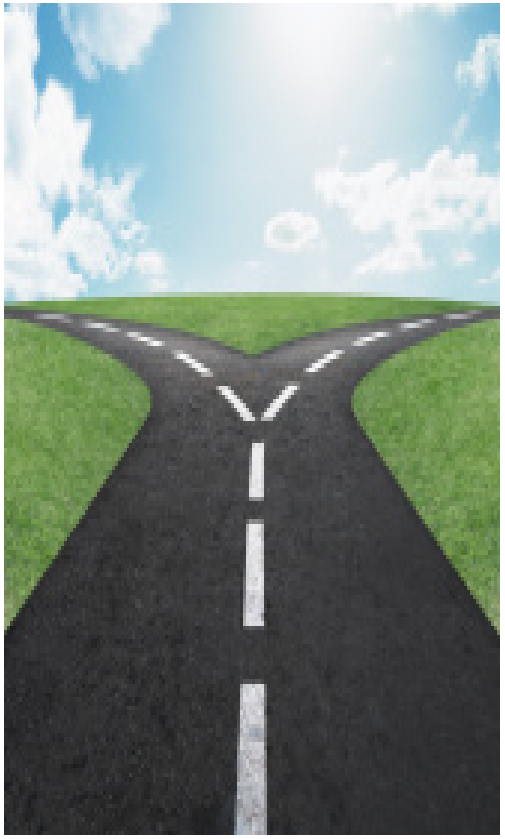
- Companies adopting clawback policies should consider the tensions:[2] (1) between rewarding proper risk-taking and disincentivizing excess risk; (2) between encouraging both compliance and the reporting of noncompliance; and (3) between providing the board with flexibility to implement the policy without inadvertently triggering adverse accounting or tax consequences.

1: PricewaterhouseCoopers LLP, Executive Compensation: Clawbacks - 2013 Proxy Disclosure Study.
2: "The Drawbacks of Clawbacks," The Wall Street Lawyer (June 2014).

Evolving Role of Chief Compliance Officers

Splitting Compliance and Legal

- A recent survey[1] indicates that 56% of NYSE companies have a dedicated compliance officer who has overall responsibility for their company's compliance program – only 8% of survey respondents indicated that this job fell to the general counsel or corporate legal officer.
- In the same survey, only 18% of respondents reported that the compliance function reports to the general counsel's office.
- The trend of separating compliance and legal functions is likely due in large part to the U.S. Federal Sentencing Guidelines, which prefer a dedicated compliance function with a reporting line, not to a corporate legal department, but to the CEO or board.
- In January 2015, a major U.S. financial institution moved its compliance function from its legal department to its risk oversight group. The move came after the company met with its regulator, the Office of the Comptroller of the Currency (OCC).

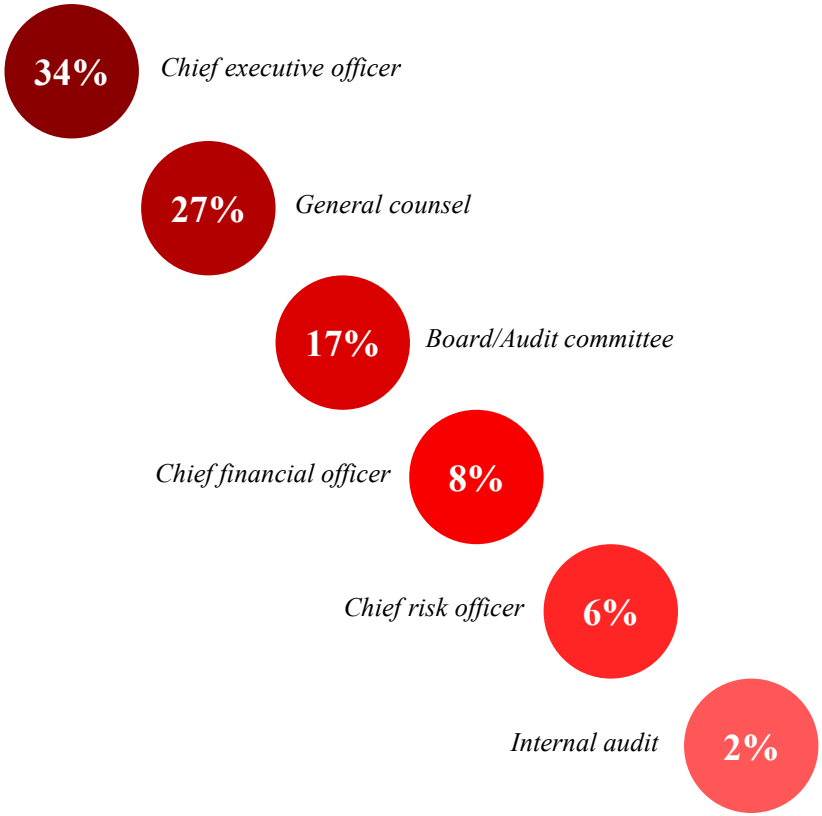


1: NYSE Governance Services 2014 Compliance and Ethics Program Environment Report; a total of 249 of the respondents included midsize to large companies.

Evolving Role of Chief Compliance Officers

Reporting Trends

To whom does the chief compliance officer report?[1]



- A recent survey[1] indicates that 88% of companies with annual revenues of $25 billion or more have chief compliance officers, and only 63% of companies with annual revenues between $1 and $5 billion have chief compliance officers.
- Organizations in heavily regulated industries are more likely to have chief compliance officers.
- Recent studies indicate that many compliance officers are still evolving into the role of a "chief," a title that implies enterprise-wide focus and integration with business operations.

1: PricewaterhouseCoopers LLC State of Compliance Survey (2014).

Shifting Pressures for Compliance Professionals

- Compliance, in-house auditors, and other "gatekeepers," in most cases, must wait at least 120 days after they have reported internally before they may report to the SEC.
- In September 2014, the SEC awarded a compliance and audit professional at a company $300,000 for providing the information that led to an enforcement action.
- The SEC and other regulatory bodies, such as the Financial Crimes Enforcement Network (FinCEN), recently have brought actions against compliance officers for failing to ensure the effectiveness of the compliance program or for altering compliance documents.
- FinCEN, in assessing a $1 million penalty against the former chief compliance officer of a money transfer company, stated that "[h]is inaction led to thousands of innocent individuals being duped out of millions of dollars through fraud schemes."
- The SEC and DOJ increasingly are asking companies and compliance professionals to "name names."

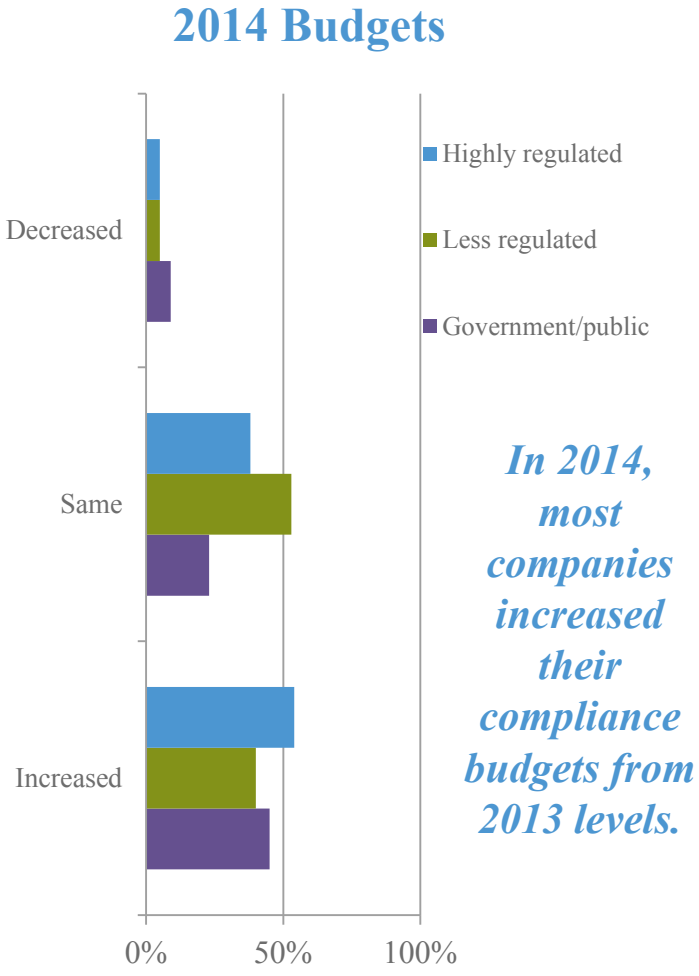
"If you want full cooperation credit, make your extensive efforts to secure evidence of individual culpability the first thing you talk about when you walk in the door to make your presentation."

– Marshall L. Miller, DOJ Principal Deputy Assistant Attorney General (Sept. 17, 2014)

Trends for Compliance Departments

Statistics on Reporting Structures and Budgets

- Corporate compliance staffing and budgets are trending up. According to a recent survey almost half (47%) of respondents indicated that compliance staffing levels have increased over the past 12 months.
- Highly regulated industries saw the most significant increases, but less regulated industries, such as retail, consumer, and automotive, also saw staffing increases in 2014. A similar pattern is reflected with respect to compliance budgets. In addition, several banks have recently announced plans to grow their compliance and risk staff.
- The representation in compliance departments is also shifting. Personnel with industry expertise and data analytics skills are being brought on board.
- Use of data analytics can help companies identify key areas of concern (e.g., high-risk suppliers, vendors subject to sanctions, emails with sensitive data).



In 2014, most companies increased their compliance budgets from 2013 levels.

GIBSON DUNN

1: PricewaterhouseCoopers LLC State of Compliance Survey (2014).

Size of Compliance Department

- Compliance groups are tailored to the scope and nature of the businesses in which they operate.
  - Compliance personnel may be deployed to different geographic areas in order to capture decision-making in real time.
  - There is no reliable metric to determine the number of compliance officers that a company should have vis-à-vis overall headcount.
- "Every employee is a compliance officer" – this is achieved through:
  - Trainings;
  - Tone from the top; and
  - Culture of integrity.

- A UK financial company substantially increased the size of its compliance and risk group following a $1.9 billion settlement with DOJ charging anti-money laundering and sanctions violations; the company's third quarter earnings call revealed that nearly 10% of its workforce work in compliance and risk.
  - The company's CEO indicated that the company spends between $750 million and $800 million per year on its compliance and risk program, and that the 2015 budget is expected to increase.

Challenges Regarding Senior and Middle Managers

- Although a recent survey by the Ethics Resource Center[1] reports that workplace misconduct is at a historic low, the survey found that managers are most often responsible for corruption-related misconduct.
- The same survey also indicates that the majority of these activities occur in non-U.S. countries, suggesting that companies still need to focus on global training efforts and establishing an enterprise-wide corporate culture of ethics.

Perpetrator	Accepting Inappropriate Gifts	Offering Bribes to Clients	Offering Bribes to Public Officials	Making Improper Political Contributions
Senior leader(s)	25%	30%	41%	53%
Middle managers(s)	27%	22%	28%	13%
First-line supervisor(s)	19%	16%	14%	11%
Non-management employee(s)	24%	25%	16%	19%
Other	6%	6%	0%	4%

1: Ethics Resource Center, National Business Ethics Survey of the U.S. Workforce (2014).

Whistleblower Update[1]

- FY14 was historic for the SEC Office of the Whistleblower (OWB), both in terms of the number and the dollar amount of whistleblower awards.
- The SEC authorized an award of more than $30 million to an overseas whistleblower who provided key original information that led to a successful enforcement action—the largest award made by the SEC's program to date.
- After the U.S., OWB received the highest number of whistleblower tips in FY14 from individuals in the United Kingdom, India, Canada, the People's Republic of China, and Australia.
- Section 21F(h)(1) of the Exchange Act, promulgated by Section 922 of the Dodd-Frank Act, prohibits employers from retaliating against individuals in the terms and conditions of their employment when they engage in whistleblowing activities.
- On June 16, 2014, the SEC exercised its anti-retaliation authority for the first time and charged a hedge fund advisory firm with retaliating against an employee for reporting prohibited principal transactions to the SEC. The firm's owner paid $2.2 million to settle the SEC's charges.

1: 2014 Annual Report to Congress on Dodd-Frank Whistleblower Program.

Internal Reporting and Anti-Retaliation Trends

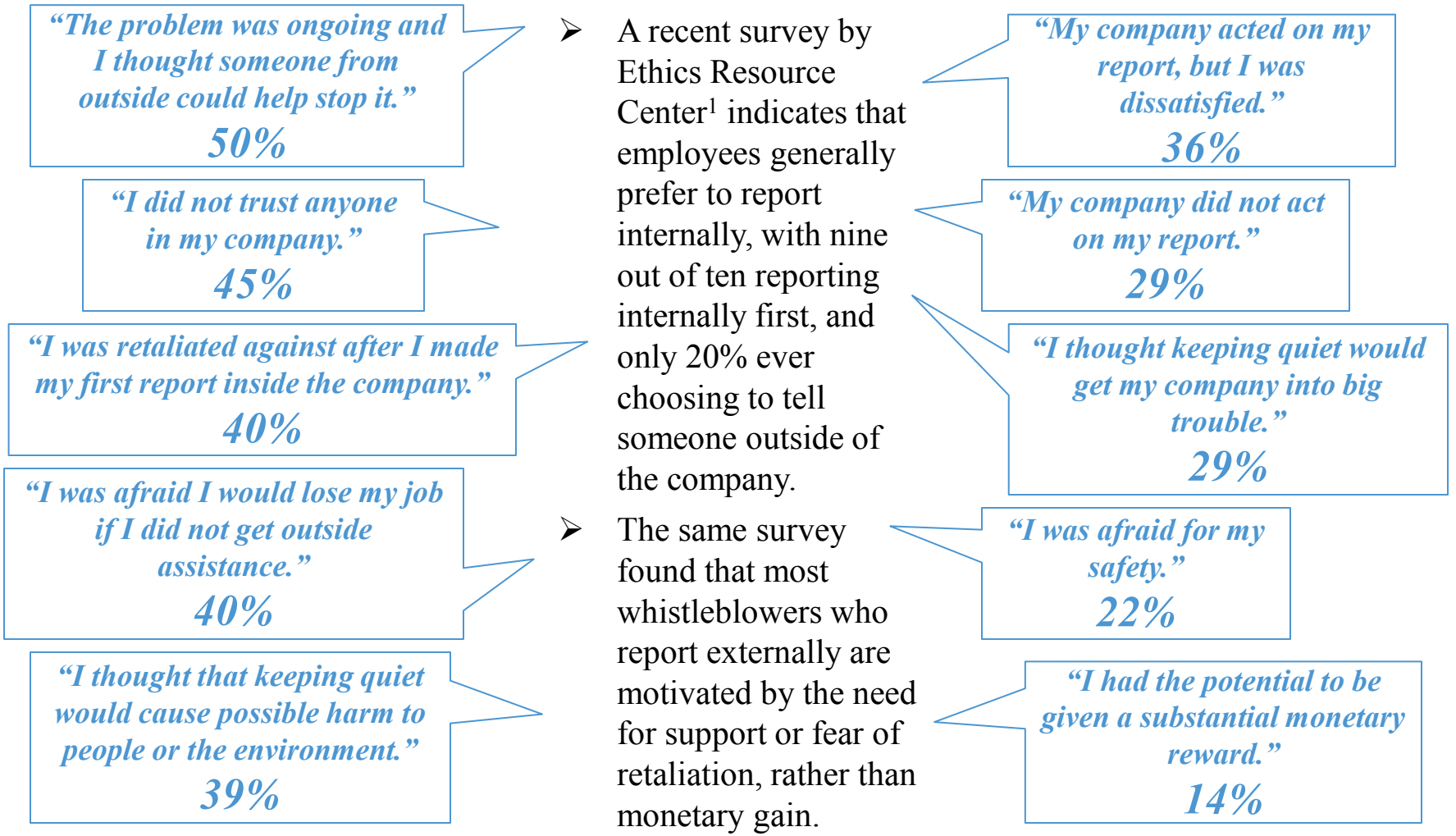
- Recent surveys indicate that at many companies, incidents of retaliation continue to creep upwards, consistent with prior years. Researchers indicate that the rate of retaliation is outpacing overall whistleblower reporting.[1]

- As anti-retaliation issues can be particularly pervasive overseas, it is critical that companies structure internal reporting in such a way as to protect foreign whistleblowers.

- On August 14, 2014, the U.S. Court of Appeals for the Second Circuit held in *Liu v. Siemens AG* that the Dodd-Frank anti-retaliation protection provisions do not apply extraterritorially, but the court did not address whether those provisions apply to purely internal reporting. In dismissing the appeal, Judge Pauley cited three missing factors that put the employee's firing beyond the reach of the anti-retaliation provision: it did not involve (1) a U.S.-based company, (2) an employee in the U.S., or (3) actions that occurred inside the U.S. Had any of these factors been present, the court might very well have decided differently.

1: Ethics Resource Center, National Business Ethics Survey of the U.S. Workforce, (2014).

Understanding Why Employees Report Out



GIBSON DUNN

1: Ethics Resource Center, National Business Ethics Survey of the U.S. Workforce (2014).

Updates on Other Current Governance Topics

- Shareholder Proposal Season: Proxy Access
- Fee Shifting and Forum Selection Bylaws

Shareholder Proposal Season: Proxy Access

- Support for proxy access rights reached a tipping point in 2014, with five proposals approved during the first half of the year. For the 13 proposals that went to a vote, average support was 39.1% of votes cast, up from 31.8% in 2013.
- Based on current estimates, nearly 1/5th of the proposals received by companies to date for 2015 shareholder meetings relate to proxy access. The NY City Comptroller (on behalf of certain pension funds) is reported as having submitted the highest number of these proposals in connection with the proxy access campaign it announced in November.
- In October 2014, Whole Foods asked the SEC to concur with the exclusion of the proxy access proposal (with a 3%, 3-year ownership threshold) on the basis of Rule 14a-8(i)(9), because the company planned to submit a conflicting proposal (with a 9%, 5-year ownership threshold) to shareholders. The SEC concurred initially, but subsequently declined to express a view.
- On January 16, 2015, the Staff issued a press release announcing that it will not issue any opinions regarding the application of Rule 14a-8(i)(9) this season because the Staff is currently reviewing and issuing a report on the rule.
- Despite the increase in proxy access proposals, shareholder proposals that pertain to sustainability issues remain the most prevalent.

Fee Shifting and Forum Selection Bylaws

- Fee-shifting bylaws impose attorney's fees on unsuccessful claimants in shareholder suits.
- In May, in *ATP Tour, Inc. et. al. vs. Deutscher Tennis Bund,* the Delaware Supreme Court concluded that a corporation may unilaterally amend its bylaws in order to make shareholders who lose their derivative suits against the corporation personally liable for legal expenses – even if those shareholders win on some of the issues for which they bring suit.
  - Critics from the plaintiffs' bar have warned that allowing fee-shifting bylaws will not just discourage frivolous litigation, but prevent litigation altogether, eliminating even meritorious claims.
  - Though ATP Tour is a private company, the holding does not exclude public companies from taking the same action, and many public companies have instituted such bylaws following the ruling.
  - Legislative proposals to overturn the ruling have thus far been unsuccessful.
- Forum selection bylaws are bylaw provisions that designate an exclusive forum for intra-corporate litigation.
- Forum selection bylaws may reduce cost, disruption, and forum shopping by plaintiffs, but may result in proxy advisor and investor criticism.

The Current Environment

The Current Environment

- Details on SEC Enforcement in 2014
- High-Profile SEC Losses
- Increasing Use of Administrative Proceedings
- Mixed Messages on "Broken Windows"
- Details on DOJ Enforcement in 2014
- DOJ Fines and Recoveries Continue to Trend Upward

Details on SEC Enforcement in 2014

Takeaways From 2014 Cases and Settlements

- SEC enforcement continues apace. In FY14, the SEC:
  - Filed a record 755 enforcement actions and obtained orders totaling $4.16 billion in disgorgement and penalties. This constitutes an increase of 69 enforcement actions and an increase of $760 million in disgorgement and penalties from FY13.
  - Promoted whistleblower activity, including awarding nine whistleblowers with total awards of approximately $35 million; and
  - Obtained its highest-ever civil penalty awards against individuals: $524,000 for each respondent (*SEC v. Uriel Sharef et al.*).
- After being put to its burden of proof on negating the applicability of the FCPA's facilitating payment exception, the SEC settled on the eve of trial with defendants James J. Ruehlen and Mark A. Jackson in what was largely perceived as a successful challenge to the SEC's ability to carry that burden (*SEC v. Ruehlen, et al.*).

"Aggressive enforcement against wrongdoers who harm investors and threaten our financial markets remains a top priority, and we brought and will continue to bring creative and important enforcement actions across a broad range of the securities markets."
– Mary Jo White, SEC Chair (Oct. 16, 2014)

High-Profile SEC Losses

- ***SEC v. Obus (S.D.N.Y., May 30, 2014)***. On May 30, 2014, a jury in the U.S. District Court for the Southern District of New York returned a unanimous verdict in favor of Nelson Obus and his co-defendants in an insider trading case involving 13-year-old facts. The SEC had alleged that Mr. Obus and his analyst, Peter Black, traded on inside information in connection with the purchase of SunSource, Inc. by their company, Wynnefield Capital, Inc. The case is an example of a well-crafted defense strategy and offers a view into the aggressive tactics mustered by the SEC when it is required to prove a case rather than settle it.
- ***SEC v. Moshayedi (C.D. Cal., June 6, 2014)***. On June 6, 2014, a jury in the U.S. District Court for the Central District of California delivered a unanimous verdict in favor of Manouch Moshayedi in one of the largest insider trading cases ever filed by the SEC. The SEC had alleged that Moshayedi engaged in insider trading and violated the anti-fraud provisions of the federal securities laws in connection with a secondary offering of approximately $267 million worth of sTec stock owned by Moshayedi and members of his family.
- Following these back-to-back trial losses, the SEC announced a plan to bring more insider-trading cases as administrative proceedings.

Increasing Use of Administrative Proceedings

- Judge Jed Rakoff (S.D.N.Y.) has expressed criticism of the SEC's increased use of administrative proceedings, as opposed to federal court trials, to resolve its enforcement actions.
- The courts have denied motions to move proceedings to federal court.
  - In a December 2014 opinion, Judge Kaplan (S.D.N.Y.) denied a motion challenging an SEC administrative proceeding as unfair, but recognized that "the growth of administrative adjudication . . . perhaps particularly in the field of securities regulation, troubles some." He acknowledged that "these concerns are legitimate."

"Just like the rest of the enforcement division, we're moving towards using administrative proceedings more frequently . . . It's fair to say it's the new normal"

– Kara Brockmeyer, SEC FCPA Unit Chief (Oct. 9, 2014)

In the 12 months through September 2014, "the SEC won all six contested administrative hearings where verdicts were issued, but only 61% - 11 out of 18 – federal-court trials, according to previously unpublished figures.

***– The Wall Street Journal* (Oct. 21, 2014)**

- In a speech in November 2014, Rakoff warned against "administrative fiat" and the "administrative creep" of the SEC's internal enforcement power, made all the more worrisome with the significant expansion of the breadth and depth of the agency's powers. This trend, he said, threatened to "hobble the balanced development of the securities laws" by circumventing the careful jurisprudence of the federal court system.

Mixed Messages on "Broken Windows"

- Internal disagreement over the "broken windows" approach to securities enforcement touted by Chair White in October 2013 became apparent at the same Securities Enforcement Forum just one year later.

"Investors do not want someone who ignores minor violations . . . they want someone who understands that even the smallest infractions have victims . . . . They deserve an SEC that looks at its enforcement mission in exactly that way . . . we are looking for the 'broken windows' in our markets."
– Mary Jo White, SEC Chair (Oct. 9, 2013)

"A 'broken windows' approach to enforcement may not achieve the desired result. If every rule is a priority, then no rule is a priority."
– Michael Piwowar, SEC Commissioner (Oct. 14, 2014)

"[The 'broken windows' approach] has increased compliance . . . tremendously"
– Andrew Ceresney, SEC Director of Enforcement (Oct. 14, 2014)

Excessive enforcement of minor violations could 'unnecessarily shackl[e]' economic activity.
– Michael Piwowar, SEC Commissioner (Oct. 14, 2014)

Details on DOJ Enforcement in 2014

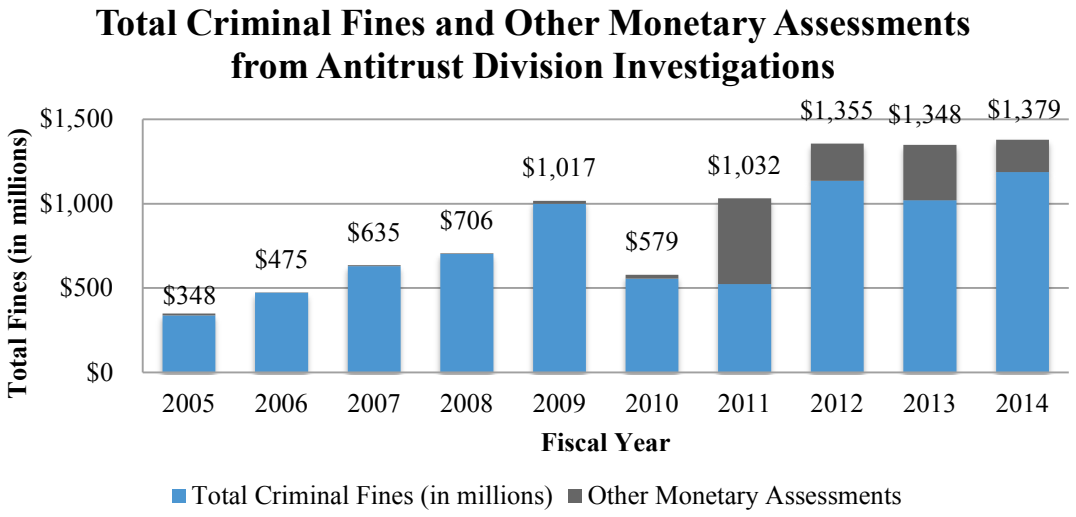
Takeaways From 2014 Cases and Settlements

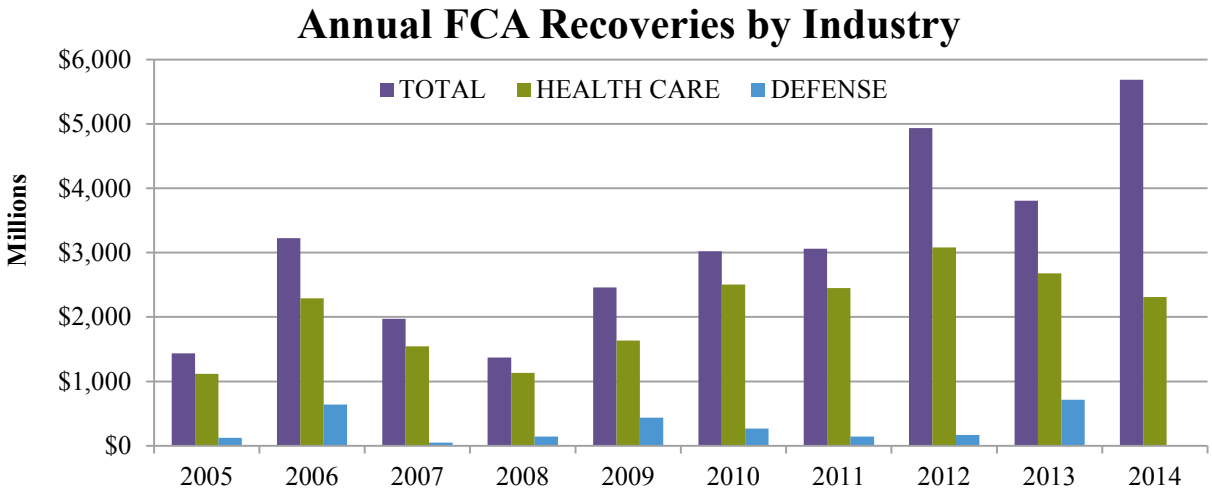
- FY14 has seen aggressive enforcement efforts by the DOJ continue, with a particular emphasis placed on cross-border cooperation of law enforcement authorities to prosecute an ever-growing number of multi-jurisdictional crimes.
- Recently, DOJ's Marshall Miller emphasized the DOJ's aggressive approach in prosecuting individual violators when he stated that companies seeking to cooperate with DOJ investigations must identify individual suspects.
- Following a collaborative and thorough review, in May 2014 Attorney General Eric Holder announced a new policy for the DOJ that creates a presumption that statements made by individuals in federal custody, following arrest but prior to their first appearance in court, will be electronically recorded.

"We must continue to grow both tougher and smarter on crime."
– Eric Holder, U.S. Attorney General (April 3, 2014)

DOJ Fines and Recoveries Continue to Trend Upward

- The DOJ obtained approximately $1.19 billion in criminal fines for violations of the Sherman Act – an all-time high.
- Over 65% of that total resulted from the $785 million in fines paid by auto-parts manufacturers in the Division's ongoing investigation into collusion in the auto parts industry.





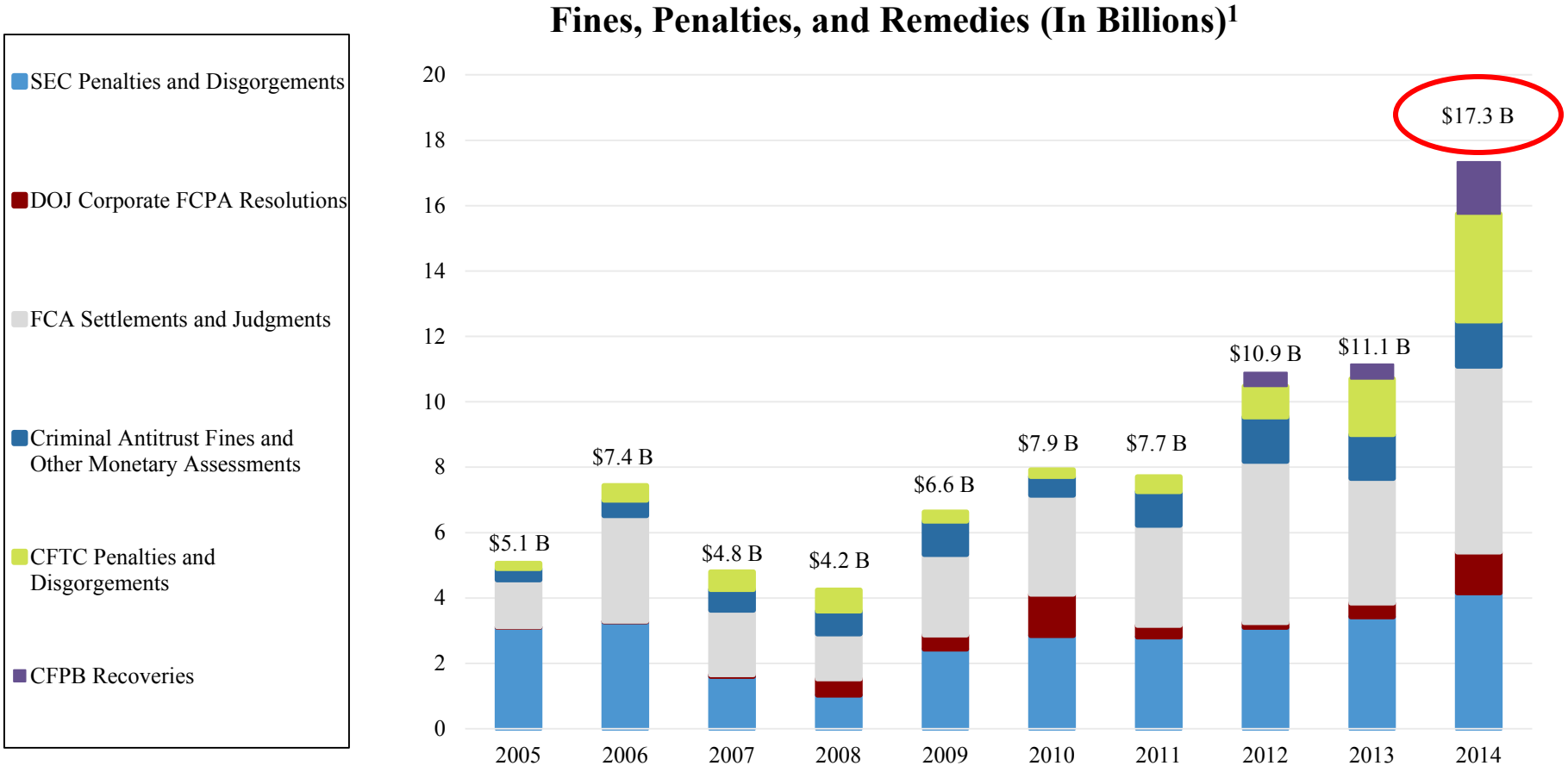
- At $5.7 billion in FY14, FCA represented the largest portion of DOJ civil recoveries, with the largest recoveries from banks ($3.1 billion).

U.S. Regulatory & Enforcement Trends

U.S. Regulatory & Enforcement Trends

- Record-Breaking Fines and Settlements
- Areas of Rising Concern:
  - U.S. Trade Sanctions Update
  - False Claims Act (FCA) Update
  - Criminal Tax Update
  - New Guidance from U.S. Department of Treasury Financial Crimes Enforcement Network (FinCEN)
  - Financial Institutions Reform, Recovery, and Enforcement Act (FIRREA) Update
- Foreign Corrupt Practices Act (FCPA) Update
- Antitrust Update
- Consumer Financial Protection Bureau (CFPB) Update
- Commodity Futures Trading Commission (CFTC) Update

Another Record Year for Fines



Total fines in 2014 were more than 50% higher than total fines in 2013, due in large part to growing areas of concern (e.g., CFTC and CFPB), as well as increased fines in established areas.

GIBSON DUNN

1: GDC Internal Aggregations.

Record-breaking Settlements

- ***Trade Sanctions***. A French bank and financial services company pled guilty to two criminal charges and agreed to pay almost $9 billion to resolve accusations that it had violated U.S. sanctions against Sudan, Cuba, and Iran.

- ***Bank Secrecy***. An international banking institution agreed to pay a total of $1.7 billion to the DOJ and $350 million to the OCC to settle allegations that the bank violated the Bank Secrecy Act by maintaining a banking relationship with Bernie Madoff.

- ***FCPA***. An energy and transport company pled guilty and agreed to pay a record $772 million to end a DOJ investigation into bribes paid to win power-plant contracts in Indonesia and the Middle East. The fine is the largest criminal penalty paid to the DOJ under the FCPA to date.

- ***FIRREA***. The DOJ reached a $16.65 billion settlement with an international financial company, the largest civil settlement with a single entity in American history, to resolve federal and state claims regarding the company's mortgage arrangements. In connection with this resolution, the company agreed to pay a $5 billion penalty under FIRREA, the largest FIRREA penalty to date.

- ***Antitrust***. An auto parts manufacturer received an unprecedented penalty for failing to voluntarily report conduct and was fined $450 million. Numerous jurisdictions are now investigating the same conduct.

Top Fines, Records, and Penalties in 2014 for Anti-Corruption, Antitrust, False Claims Act, and Sanctions Offenses

Amount	Industry	Area	Date
$1.85 billion*	Finance	False Claims Act	08/21/2014
$1.02 billion	Finance	Market Manipulation	11/12/2014
$1.01 billion	Finance	Market Manipulation	11/12/2014
$963.6 million**	Insurance	Sanctions	06/30/2014
$799 million	Finance	Market Manipulation	11/12/2014
$772.3 million	Energy & Transport	Anti-bribery (FCPA)	12/22/2014
$634 million	Finance	Market Manipulation	11/12/2014
$618 million	Finance	Market Manipulation	11/12/2014
$614 million	Finance	False Claims Act	02/04/2014
$489 million	Healthcare	Anti-bribery (China)	09/19/2014
$434.4 million	Logistics	False Claims Act / Fraud	12/08/2014
$418 million***	Finance	False Claims Act	06/17/2014
$425 million	Manufacturing	Antitrust	02/13/2014
$384 million	Metals	Anti-bribery (FCPA)	01/09/2014
$370 million	Finance	Antitrust (LIBOR)	07/28/2014
$350 million	Healthcare	False Claims Act	10/22/2014
$315 million	Finance	Banking / Sanctions	11/18/2014

* Part of an overall $16.65 billion settlement to resolve federal and state claims.
** Part of an overall $8.9 billion settlement with various state and federal agencies.
*** Part of an overall $968 million settlement with various state and federal agencies.

U.S. Economic and Trade Sanctions Legal Regime

- The U.S. economic and trade sanctions legal regime is administered and enforced by the Department of the Treasury, Office of Foreign Assets Control (OFAC).
- OFAC's authority is derived from a number of statutes:
  - For most sanctions, the International Emergency Economic Powers Act, 50 U.S.C. §§ 1701-06 (IEEPA);
  - Iran has special sanctions provisions enacted through the Iran Sanctions Act of 1996 (codified in IEEPA), and modified by the Comprehensive Iranian Sanctions and Divestment Accountability Act of 2010, 22 U.S.C. 8501 (CISADA) and the Iran Threat Reduction and Syria Human Rights Act of 2012 (TRA);
  - For the longstanding Cuban embargo, the Trading with the Enemy Act, 50 U.S.C. App. §§ 1-44 (TWEA);
  - Several other statutes that often overlap and buttress each other, including those with specific provisions covering narcotics trafficking and terrorism.
- Sanctions laws are principally implemented through Presidential Executive Orders and in Chapter V of C.F.R. Title 31.

U.S. Economic and Trade Sanctions Legal Regime

- There are over two dozen separate OFAC sanctions programs, each with varying specific restrictions.
  - ***Country-based***. Broad-based restrictions on dealing with that country's government, natural and legal persons in that country, and in some cases, goods from that country, or nationals of that country wherever located.
    - Includes: Cuba, Iran, Sudan, Syria, and to a lesser extent, Myanmar (only certain commodities) and N. Korea (import restrictions only).
  - ***List-based***. Individuals and entities designated for engaging in various illicit activities, such as narcotics trafficking, WMD proliferation, undermining democracy, human rights abuses and other violations of international law.
    - Prominent lists include: Specially Designated Nationals (SDN) List; Foreign Sanctions Evaders (FSE) List, and Sectoral Sanctions Identifications (SSI) List.
- OFAC sanctions operate under a strict liability standard, with no materiality or *de minimis* requirements.

Scope of OFAC Sanctions

- OFAC applies to all "U.S. persons" (natural and legal), which is defined to include:
  - U.S. citizens and permanent resident aliens, wherever located;
  - Entities organized under the laws of the U.S., including foreign branches; and
  - Any person in the U.S., including branches and subsidiaries of foreign entities.
- Most OFAC sanctions do not apply to foreign subsidiaries of U.S. companies.
  - Exceptions: Iran and some Cuba restrictions.
- Restrictions may apply to foreign persons in certain circumstances:
  - IEEPA makes it illegal to "cause" a violation of trade sanctions, which could apply to an activity of a foreign entity that causes a U.S. entity to violate OFAC sanctions.
  - Iran sanctions apply to foreign financial institutions for certain restricted activities.

General Prohibitions

- U.S. persons generally are prohibited from:
  - Transacting, directly or indirectly through intermediaries, with a sanctioned country, individual or entity, with their property or their interests in property;
  - Transacting with an entity owned 50% or more, individually or in the aggregate, directly or indirectly by, one or more persons on the SDN List;
  - Facilitating a transaction which would be prohibited if performed by a U.S. person; and
  - Attempting or conspiring to violate or evade U.S. sanctions.
- Any property of an SDN is "blocked" and must be frozen if it comes into possession of a U.S. person.
  - Transactions with other persons may also be blocked or merely prohibited (requiring the U.S. person to reject the transaction), depending on the specific sanctions program.
- SSI-listed entities are subject to specified restrictions but are not automatically blocked.

OFAC Penalties

- ***Civil Monetary Penalties***. Base penalty assessed per violation as follows:

		Egregious Case?	
		No	*Yes*
Voluntary Self-Disclosure?	*Yes*	1/2 the transaction value (capped at $125,000 per IEEPA violation/$32,500 per TWEA violation)	1/2 the statutory maximum ($125,000 under IEEPA/$32,500 under TWEA)
	No	Schedule amount (capped at $250,000 per IEEPA violation/$65,000 per TWEA violation)	Statutory maximum ($250,000 under IEEPA/$65,000 under TWEA)

- ***Criminal Penalties***. IEEPA and TWEA contain criminal provisions, and although OFAC will not itself pursue criminal enforcement, it may refer the matter to other federal authorities.
  - *IEEPA*: $1 million fine, 20 years imprisonment or both.
  - *TWEA*: $1 million fine ($100k for individuals), 10 years imprisonment or both.

U.S. Trade Sanctions Update

Select Enforcement Actions

- ***A European clearing house.*** The company agreed to remit approximately $152 million to settle claims by OFAC that the company allegedly violated the Iranian Transactions and Sanctions Regulations (ITSR) by maintaining an account in which the Central Bank of Iran maintained a beneficial ownership interest.
- ***An aerospace services provider***. The company settled with OFAC for approximately $51 million for allegedly violating the ITSR, and the Sudanese Sanctions Regulations (SSR), 31 C.F.R. part 538, by indirectly exporting spare aircraft parts to Iran and to Sudan from November 2005 to September 2010.
- ***A professional services firm***. The New York Department of Financial Services (DFS) entered into a settlement agreement with the company for $25 million for its role in allegedly misrepresenting facts to regulators in connection with a previous investigation that led to a consent order with a financial institution.
- ***A financial institution***. DFS also fined the financial institution $315 million for its alleged role in convincing the professional services firm to alter the contents of its report.

U.S. Trade Sanctions Update

Ukraine and Russia

- Executive Order 13,660, "Blocking Property of Certain Persons Contributing to the Situation in Ukraine" broadly targets pro-Russia, pro-separatist elements in Ukraine;
- Executive Order 13,661, "Blocking Property of Additional Persons Contributing to the Situation in Ukraine" focuses on officials of the Government of the Russian Federation and persons operating in the arms or related sectors in the Russian Federation;
- Executive Order 13,662, "Blocking Property of Additional Persons Contributing to the Situation in Ukraine" authorizes sanctions on any person determined by the Secretary of the Treasury to operate in particular sectors of the Russian Federation economy, such as financial services, energy, metals and mining, engineering, and defense;
- Executive Order 13,685, "Blocking Property of Certain Persons and Prohibiting Certain Transactions with Respect to the Crimea Region of Ukraine" prohibits exports to and imports from Crimea of goods, technology and services, as well as new investment in Crimea;
- OFAC issued a number of Directives that placed sanctions on a number of Russian entities in the financial services, energy, and defense sectors, and restricted U.S. entities from conducting certain transactions with such Russian entities; and
- The Support for Sovereignty, Integrity, Democracy, and Economic Stability of Ukraine Act of 2014 provides for certain recovery of assets, enhanced democracy and security measures in Ukraine and the region, and targeting sanctions at persons responsible for violence or corruption in the area.

U.S. Trade Sanctions Update

Global Review

- ***Cuba***.
  - In January 2015, the U.S. Treasury and Commerce Departments revised their regulations to expand permissible trade and travel involving Cuba.
  - Though the broader U.S. embargo against Cuba remains in place and normal tourism is still prohibited, the announced policy shift will result in substantial changes to the implementation of the embargo, the ability of individuals to travel between the two countries, and the ability of U.S. businesses to engage in limited commerce with the Cuban people.
- ***South Sudan***. Executive Order 13,664, "Blocking Property of Certain Persons with Respect to South Sudan" declared a national emergency to deal with the "threat to the national security and foreign policy of the United States" resulting from violence and instability in South Sudan.
- ***Central African Republic***. Executive Order 13,667, "Blocking Property of Certain Persons Contributing to the Conflict in the Central African Republic" declared a national emergency based on the "breakdown of law and order, intersectarian tension, widespread violence and atrocities, and the pervasive, often forced, recruitment and use of child soldiers" in the Central African Republic.

U.S. Trade Sanctions Update

Global Review, Continued

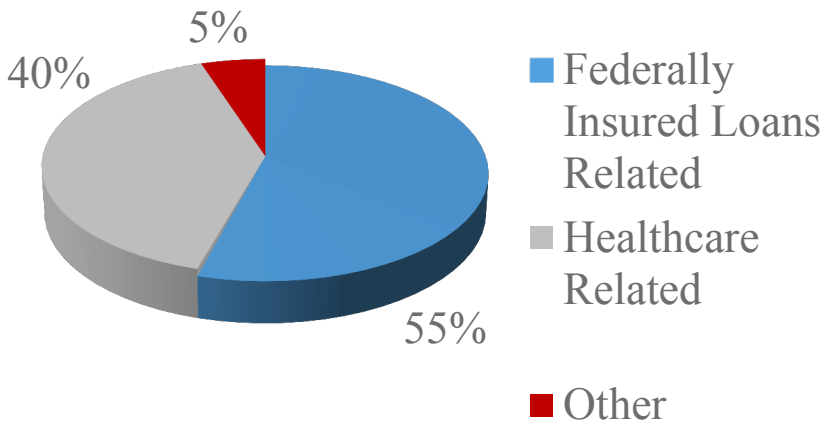
- ***Iraq***. Executive Order 13,668, "Ending Immunities Granted to the Development Fund for Iraq and Certain Other Iraqi Property and Interests in Property Pursuant to Executive Order 13303, as Amended" terminated the immunities originally instituted in 2008 from the judicial process for assets of the Development Fund for Iraq, Iraqi petroleum and petroleum products, and the Central Bank of Iraq. Order 13,668, however, maintained the national emergency declared back in 2008.
- ***Democratic Republic of the Congo***. Executive Order 13,671, "Taking Additional Steps to Address the National Emergency With Respect to the Conflict in the Democratic Republic of the Congo," was issued in response to "the continuation of activities that threaten the peace, security, or stability of the Democratic Republic of the Congo and the surrounding region, including operations by armed groups, widespread violence and atrocities, human rights abuses, recruitment and use of child soldiers, attacks on peacekeepers, obstruction of humanitarian operations, and exploitation of natural resources to finance persons engaged in these activities[.]" Executive Order 13,671 amended Executive Order 13,413 signed by President Bush in October 2006, to broaden the bases for designating SDNs.

Sanctions: Compliance Takeaways

- Pay close attention to sanctions programs that are changing, whether restrictions are tightening or relaxing. Take care to not overstate sanctions reduction.
- Perform reasonable, but adequate diligence concerning ownership.
- Consider carefully the scope of the applicable restrictions on SSI-listed entities – some entities may be subject to multiple Directives.
- Exercise caution in dealing with SSI-listed entities or entities owned less than 50% by SDNs as they may be candidates for future designation on the SDN List.
- Maintain a robust and up-to-date compliance and screening program.

FCA Statistics and Key Trends

- ***FY14 Statistics:***
  - The DOJ recovered $5.69 billion from FCA settlements and judgments in FY14, a new record.
  - $3.1 billion of this total came from banks and other financial institutions involved in federally-insured mortgages and loans.
  - Qui tam suits accounted for $3 billion, of which the whistleblowers received $435 million.

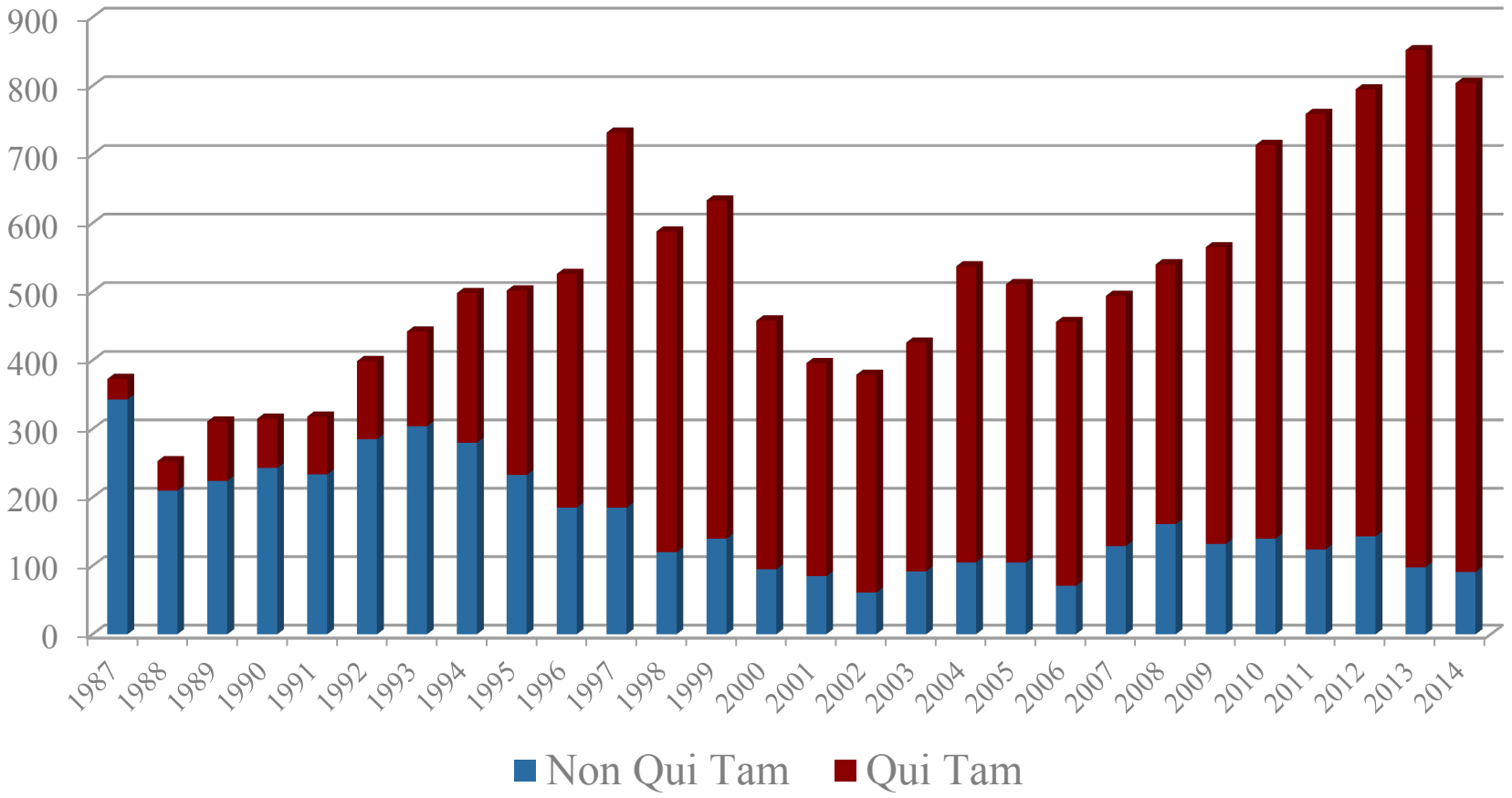


- ***Trends:***
  - Most of DOJ's monetary recovery under the 1986 amended statutes has come in last three years.
  - More than 700 qui tam suits were filed in each of FY14 and FY13.
  - New DOJ Criminal Division procedure investigates all qui tam suits as soon as they are filed to decide whether to begin a parallel criminal investigation.

Update on Substance of FCA Theories

- ***Medical Necessity:***
  - In 2014, the government vigorously utilized the theory that defendant providers had billed for medically unnecessary or unreasonable services. This allegation was raised in more than 60% of provider settlements.
    - In April, one of the largest national home healthcare providers paid $150 million to resolve allegations that it had billed services that were medically unnecessary between 2008 and 2010, and that it had misrepresented its patients' conditions in order to increase its reimbursements from the government.
    - In August, an acute care hospital operator paid over $98.1 million to resolve government claims that it had overbilled for inpatient services.
- ***Worthless Services:***
  - The sub-standard or "failure" of care theory posits that a provider sought reimbursement for services so poor that they were effectively worthless to their recipient. The Seventh Circuit addressed the use of the theory this year in *United States* ex rel. *Absher v. Momence Meadows Nursing Center, Inc.*, holding that the theory is tenable only where the defendant's services were literally valueless. However, this theory isn't necessarily worthless – in October, the DOJ settled a case with a long-term care company for $38 million that it advertised as a win for the theory.

False Claims Act – Annual New Matters:1987 to 2014



Criminal Tax Update

- The DOJ Tax Division, in concert with the Swiss federal prosecutor, administers the "Program for Non-Prosecution Agreements or Non-Target Letters for Swiss Banks," a program that rewards participating Swiss banks that "have reason to believe [they] may have committed [certain] tax-related offenses" in connection with "U.S. Related Accounts" (as defined by the program) with NPAs for their cooperation and payment of penalties. The program is not available to the 14 banks that were already under investigation.

- A global financial services holding company agreed to pay $2.6 billion in May 2014 to settle charges made in connection with the DOJ's investigation of Swiss wealth managers. More than 100 Swiss banks are currently under investigation.

- According to the lawyers representing Swiss banks, the U.S. is eager to move on to scrutinize other offshore jurisdictions such as the Bahamas, Hong Kong, and Singapore, including subsidiaries of Swiss banks operating in such locations.

- Dozens of settlements are expected in connection with the NPA program in 2015.

New FinCEN Guidance

- On August 11, 2014 FinCEN issued an advisory to U.S. financial institutions on "promoting a culture of compliance" as it relates to institutions' anti-money laundering (AML) and Bank Secrecy Act (BSA) compliance programs.
- The advisory states that a financial institution can strengthen its BSA/AML compliance programs by ensuring that: (1) the institution's "leadership actively supports and understands compliance efforts;" (2) the institution does not let revenue interests compromise "efforts to manage and mitigate BSA/AML deficiencies;" (3) "relevant information from the various departments within the organization is shared with compliance staff;" (4) "the institution devotes adequate resources to its compliance function;" (5) "the compliance program is effective by, among other things, ensuring that it is tested by an independent and competent party;" and (6) the institution's "leadership and staff understand the purpose of its BSA/AML efforts and how its reporting is used."
- A recent survey finds that increasing regulatory action having to do with AML initiatives have led financial institutions to shift their AML function from occupying a standalone position in the compliance department to "an increasingly complex and overarching function cutting across legal, risk, operations, and tax."[1]

1: KPMG Global Anti-Money Laundering Survey 2014.

FIRREA Update

- ***Key Trends:***
  - Southern District of New York Judge Rakoff is the first to interpret how to calculate the FIRREA penalty provision.
  - The DOJ is using FIRREA to investigate subprime auto loans through subpoenas to auto finance companies.
  - The DOJ's broad civil investigation power under FIRREA could aid DOJ criminal investigations through permitted evidence-sharing between the agency's civil and criminal enforcement divisions.
- ***United States ex rel. O'Donnell v. Countrywide Home Loans, Inc:***[1]
  - Judge Rakoff imposed a $1.3 billion penalty, calculated using the gross gain measure as opposed to the net gain measure used in FCA and other civil damages methodologies.

Discussing* Countrywide, *"This is the first case in which a bank or any of its executives has been found liable under FIRREA for mortgage fraud leading up to the financial crisis, and now it is the first case in which civil penalties have been imposed upon a bank or any of its executive following such a finding. . . . This Office will continue to investigate and vigorously prosecute mortgage fraud in all of its forms using all of the civil and criminal tools at its disposal."
– Preet Bharara, U.S. Attorney Southern District of New York (July 30, 2014)

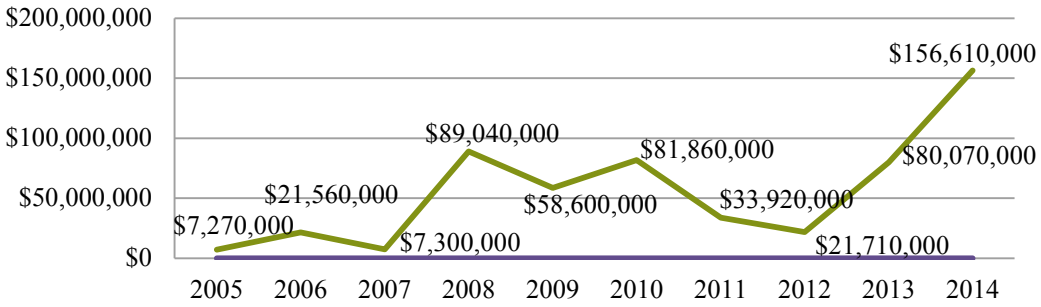
1: No. 12-cv-1422 (JSR), 2014 WL 3734122 (S.D.N.Y. July 30, 2014).

FCPA (SEC and DOJ) Statistics

2014 Fines and Penalties

- In all, the DOJ brought 17 enforcement actions against corporations and individuals, two less than it did in 2013. The SEC brought nine enforcement actions, one more than it did in 2013.
- The fifth highest monetary settlement in FCPA history was imposed on an aluminum producer at the beginning of the year. The company paid $384 million to resolve the allegations. Alstom's settlement ended the year on an even more expensive note. At $722 million, the Alstom settlement is the DOJ's biggest win to date.
- In 2014, companies paid an average $157 million to settle FCPA investigations, almost twice as much as they did in 2013, when the average settlement was $80 million.

Average Total Value of Monetary Resolutions in Corporate FCPA Enforcement Actions



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

336 Total FCPA Enforcement Actions: 2005 - 2014

FCPA (SEC and DOJ) Key Trends

Corporate Cooperation and Individual Culpability	➢ Corporate cooperation is taken into consideration in charging and settlement decisions. For example, PetroTiger voluntarily disclosed a bribery scheme by senior management to secure a Colombian oil services contract, and the agency filed no charges against the company (although charges were brought against personnel).
Instrumentality	➢ The FCPA prohibits corrupt payments to "foreign officials," a broad term which includes the personnel of an "instrumentality" of a foreign government. In May 2014, the U.S. Court of Appeals for the Eleventh Circuit held that "instrumentality" would be determined by a fact-based inquiry – an "instrumentality" is an entity (1) "controlled by the government of a foreign country" that (2) "performs a function the controlling government treats as its own." (*United States vs. Esquenazi, et al.*).
Crime/Fraud Exception	➢ In November 2014, the Supreme Court declined to review the ruling of the U.S. Court of Appeals for the Third Circuit in *In Re: Grand Jury Subpoena* that the crime/fraud exception to the attorney-client privilege may be applied in the FCPA context. The Supreme Court's decision not to take the case left a circuit split intact.

61st FCPA Opinion Procedure Release

- The DOJ released the 61st FCPA opinion procedure release (14-02) on November 7, 2014.
- The requestor, a multinational company headquartered in the U.S., intended to acquire a foreign company as its wholly-owned subsidiary.
- During due diligence of the target company, the requestor discovered a number of likely improper payments from the target company to government officials of a foreign country. None of the payments had a jurisdictional nexus to the U.S. The requestor also discovered weaknesses in target company accounting and recordkeeping.
- The requestor planned to take pre-closing remedial measures and integrate the target company into the requestor's compliance and reporting structure within a year of the acquisition.
- The DOJ confirmed that it does not plan to take enforcement action, citing the FCPA Guide's discussion on successor liability.

"Successor liability does not, however, create liability where none existed before. For example, if an issuer were to acquire a foreign company that was not previously subject to the FCPA's jurisdiction, the mere acquisition of that foreign company would not retroactively create FCPA liability for the acquiring issuer."

– DOJ, FCPA: A Resource Guide to the U.S. Foreign Corrupt Practices Act (2012)

ISO Anti-Bribery Management Standard

- The International Organization for Standardization (ISO) is currently developing a new voluntary standard on anti-bribery management, to be called ISO 37001.
- According to ISO, the standard "will help establish that the organization has implemented reasonable and proportionate measures designed to prevent bribery. These measures include leadership from the top, training, risk assessment, due diligence, financial and commercial controls, reporting, audit and investigation."[1]

"Once the future ISO 37001 is in place, as a compilation of international best practice in anti-bribery, companies will be able to apply uniform measures to prevent and detect bribery, irrespective of the countries in which they operate."

– A partner at a leading accounting firm

- ISO 37001 is being developed in a similar format to other management systems standards. The hope is for the standard to be easily recognizable by many companies and implemented in much the same way as other successful management systems.
- The ISO model is to develop the standard, but leave certification to external bodies. Which external bodies will be certifying for ISO 37001 is unclear at this stage.
- Reports indicate that a final version may be available in 2016.

1: "New Business Tool for Anti-Bribery," Elizabeth Gasiorowski-Denis, ISO News (Nov. 11, 2014)..

Antitrust Update

- Auto-parts suppliers are being simultaneously investigated by close to a dozen jurisdictions. To date, these investigations have resulted in nearly $5 billion in fines and over 20 Japanese nationals presently serving jail sentences in the U.S.

- In November 2014, financial regulators in the U.S. and Switzerland reached settlements with six banks over their alleged involvement in the manipulation of foreign exchange markets. The combined fines, penalties, and disgorgement assessed on the banks was $4.3 billion.

- Assistant Attorney General Bill Baer and his Deputy Brent Snyder at the Antitrust Division of the Department of Justice have recently reaffirmed the Antitrust Division's reluctance to credit compliance programs when considering whether to bring criminal charges against a company. The Antitrust Division's position is that the unique benefits of its voluntary leniency program will incentivize companies to implement effective compliance programs that detect the conduct first.

Antitrust Update

Extradition

- In 2014, the Antitrust Division bolstered its reputation for prosecuting individuals by obtaining the extradition of two individuals, including the first ever for an antitrust offense.
  - In April, Romano Pisciotti, an Italian businessman, became the first person to be extradited for an antitrust offense, anywhere in the world.
    - It has been reported that the U.S. authorities used a sealed indictment to place Pisciotti on an INTERPOL Red Notice, which led to his detainment in German customs.
    - Upon his extradition to the U.S., Pisciotti pled guilty to the charges and is currently serving a two-year prison sentence.
  - John Bennett was extradited from Canada to the U.S. to face charges in connection with a fraud and bid-rigging scheme involving federal contracts to clean up hazardous waste sites.
- Pisciotti's and Bennett's extraditions from Germany and Canada are further evidence of a developing network of cooperation and coordination among authorities.

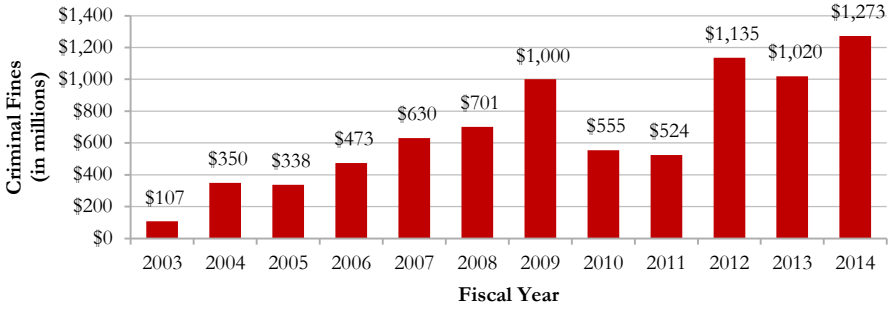
Antitrust Update

Trends in Fines and Sentences

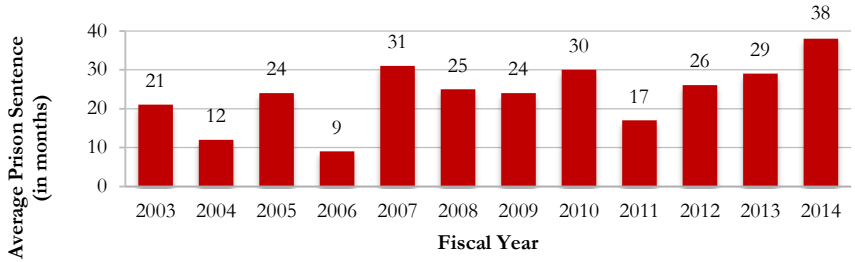
Objectives of the Antitrust Division:

- To impose large fines to encourage future corporate compliance and significant jail sentences to achieve maximum deterrence;
- To develop a global cooperation network of enforcement agencies to eliminate safe harbors where cartel members can target the U.S. economy from outside its borders; and
- To develop a convergence with other competition enforcers as well as the business community on how best to incentivize compliance and self-reporting. Nearly every competition authority in the world has followed the Antitrust Division in adopting leniency programs.

Total Criminal Fines from Antitrust Division Investigations (FY 2002–2013)



Average Length of Prison Sentence (FY 2003–2014)



GIBSON DUNN

CFPB Statistics and Key Trends

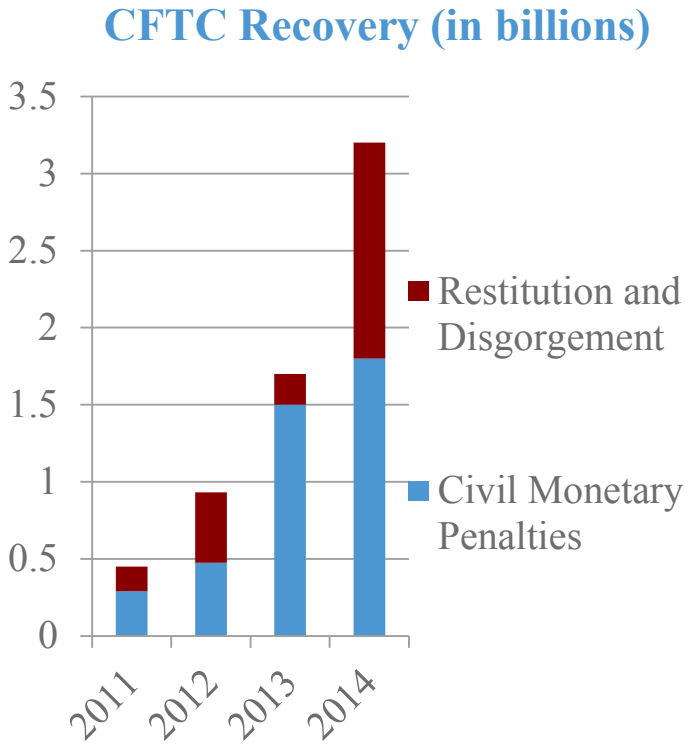
"[T]he [CFPB] now has the ability to oversee the activities of participants, whether chartered or not, in the markets for mortgage origination, mortgage servicing, private student loans, student loan servicing, payday lending, debt collection, credit [card] reporting, and international money transfers. This . . . represents a huge transformation."

– Richard Cordray, CFPB Director (Oct. 24, 2014)

- ***FY14 Statistics:***
  - The CFPB brought 41 cases and recovered more than $1.6 billion using its enforcement authority.
- ***Trends:***
  - The CFPB became fully staffed for the first time, and began a plan to normalize its supervision and examination efforts.
  - The CFPB is committed to branching out to other industries:
    - Announced action to shut down two student debt relief agencies in December 2014; and
    - Proposed new disclosures for prepaid cards in November 2014.
  - The CFPB takes an expansive view of its jurisdiction:
    - Expects non-banks to have compliance systems similar to deposit-taking financial institutions; and
    - Indicating that no industry that deals in any manner with credit, debt, or financial services, no matter how incidentally, is beyond the reach of its authority.

CFTC Statistics and Outlook

- ***FY14 Statistics:***
  - The CFTC Division of Enforcement filed 67 new cases.
  - Sanctions totaled a record $3.27 billion, compared to $1.7 billion in FY13:
    - $1.8 billion in civil penalties; and
    - $1.4 billion in restitution and disgorgement.
  - There were 240 new investigations in FY14, compared to 290 investigations in FY13 and 350 in FY12.
  - CFTC sanctions totaled more in past two years than in prior ten years combined.
- ***FY15 Outlook:***
  - The CFTC plans to conduct more of its cases before administrative law judges.
  - The CFTC is increasingly cooperating with foreign regulators and scrutinizing banks who move trading operations internationally.



International Regulatory & Enforcement Trends

International Regulatory & Enforcement Trends

- Updates by Jurisdiction
  - United Kingdom
  - European Union
  - China
  - Brazil
  - Other International Efforts
- International Cooperation

United Kingdom Enforcement Update

Serious Fraud Office (SFO)

- The SFO secured its first convictions (albeit for private corruption) under the UK Bribery Act 2010.
- The SFO also secured its first contested conviction for international corruption (before securing its second, third, fourth, and fifth convictions) – including the first contested conviction of a company – under the Bribery Act's predecessor statute.
- The SFO likely will be buoyed by these results, and with a number of high-profile investigations and prosecutions ongoing, there is every reason to expect similar results in 2015.

Financial Conduct Authority

- In December 2014, the Financial Conduct Authority (FCA) announced a major internal restructure and strategic shift in the way that it will supervise authorized firms.
- This shift by the FCA is likely to mean that many firms that might have benefited from a "lighter touch" strategy in the past should expect greater supervisory scrutiny in the future, depending on the activities they carry out and the key risks of the day.
- For many firms, this will mean that their supervisory interactions with the FCA will become more event-driven and based on thematic work.

European Union Update

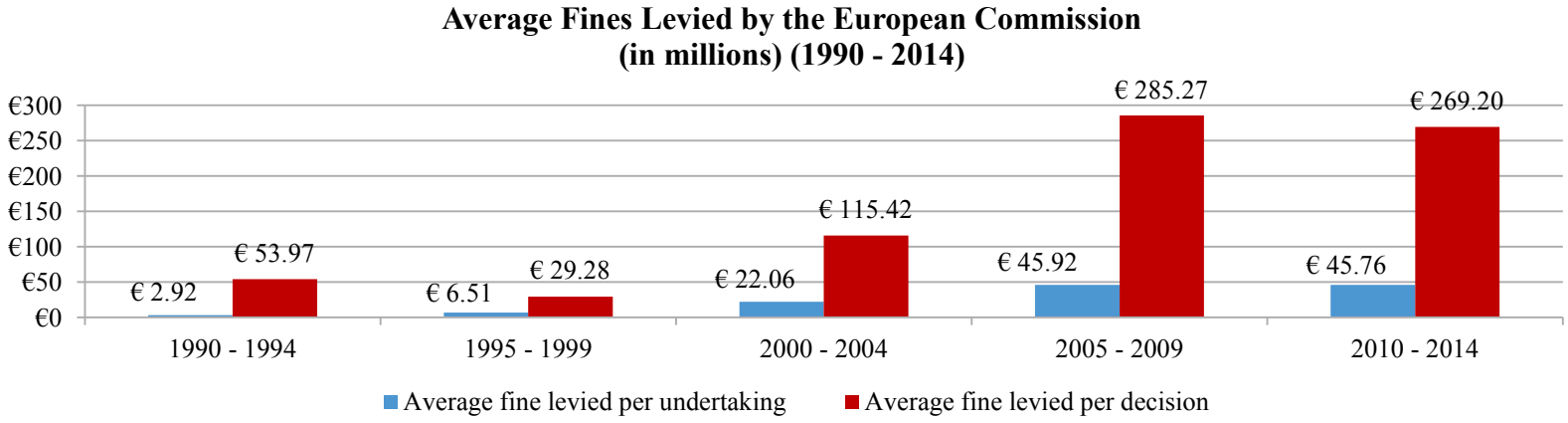
Sanctions

- The EU has adopted new or amended existing sanctions with regard to a number of jurisdictions during 2014. While the majority of the amendments concern updates of existing sanctions, for a number of jurisdictions developments have been of a more substantive nature, including the adoption of wholly-new sanction regimes for:
  - *Ukraine/Russia*: The EU repeatedly took action during 2014 in response to the escalation of the political crisis in Ukraine and in light of the EU's concern over reports on human rights violations, violence, intimidation, and missing persons. The EU's sanctions consist of: (1) misappropriation sanctions, (2) designations of those threatening Ukrainian territorial integrity, (3) economic sanctions regarding Crimea and Sevastopol, and (4) targeted sectoral sanctions against Russia.
  - *Yemen*: In July 2014, the EU implemented the UN's sanctions regarding Yemen, which impose asset freezes and travel bans on former President Ali Abdullah Saleh, as well as certain military leaders.
  - *South Sudan*: The EU imposed sanctions targeting persons obstructing the political process and persons responsible for serious violations of human rights. In particular, the EU introduced an arms embargo and prohibitions on the provision of arms-related technical assistance, brokering or other services, financing or financial assistance, or participation in activities aimed at circumventing the sanctions.

European Union Update

Antitrust

- In 2014, the European Commission (EC) levied over €1.67 billion (nearly $2.3 billion) in cartel fines, marking the third straight year that the EC topped $2 billion in fines. The risk of catastrophic sanctions has resulted in an increase in the percentage of companies that enter into voluntary settlement agreements with the EC.
- Private damages litigation has continued to rise in Member States. A November 2014 ruling by the Brussels Commercial Court dismissing the first-ever follow-on damages action brought by the EC shows that national courts may not always be receptive to private damages claims.



China Update

- ***Anti-Corruption:***
  - China grabbed global headlines this year with its prosecution and conviction of the Chinese subsidiary of a British pharmaceutical company.
  - President Xi's anti-corruption campaign continues to expand in duration and scope. From January to September 2014, more than 13,000 Chinese officials were convicted of corruption and bribery.
  - In July 2014, the Public Security Ministry launched "Operation Fox Hunt," a six-month campaign to hunt down corrupt public officials who have fled overseas, along with their stolen assets. The Ministry's estimates are staggering—18,000 corrupt officials are believed to have spirited nearly $129 billion from China.
- ***Antitrust*:**
  - China may be increasing scrutiny of multinational companies, though Chinese authorities insist they enforce the law equally. Overseas companies paid more than three-quarters of the $455 million in antitrust penalties handed down between 2011 and August 2014.
  - China's antitrust enforcement regime has been under close scrutiny and subject to criticism by the private bar, international businesses, and the internal enforcement community over the last year because of concerns that its antitrust laws lack transparency.

Brazil Update

- ***Anti-Corruption*:**
  - Brazil's new anti-bribery law has garnered significant attention from companies operating there, which now are subject to corporate criminal liability and compliance requirements.
  - In December 2014, Brazilian prosecutors charged 36 individuals with bribery, money laundering, and cartel-related offenses arising out of the highly-publicized investigation of corruption at an energy corporation, and three other individuals in connection with a separate prong of the investigation.
  - In August 2014, Brazilian authorities filed a criminal complaint accusing eight current or former employees of an aerospace conglomerate of paying a $3.5 million bribe to a Dominican Republic Air Force official in connection with a $92 million contract to deliver attack planes.
- ***Antitrust*:** In May 2014, Brazil's competition authority, CADE, imposed what are arguably the harshest sanctions ever imposed in a cartel case anywhere. CADE fined six companies, six individuals, and three industry associations involved in a suspected cement cartel a record BRL 3.1 billion ($1.3 billion). On top of the record fines, CADE also ordered the companies to divest any cross-shareholdings and reduce their concrete service assets by 20% in certain markets, and barred the defendants from cooperating on projects or buying assets from one another for five years.

Details on Other International Efforts

- Despite the country's anti-corruption rhetoric, corruption continues. The head of the Russian National Anti-Corruption Committee, a civic organization established to eradicate corruption in Russia, claims that nearly 30% of Russian government officials are corrupt, and that the problem is the direst in the public procurement sector.

- In October 2014, the new Ukrainian government adopted a series of anti-corruption laws, which define the mandates of the country's new anti-corruption and enforcement agencies.

- In September 2014, the German Criminal Code was amended to include a new statutory offense, "Passive and Active Bribery of Members of Legislative Bodies." The revised offense expands prohibited conduct to include the provision of immaterial benefits.

- After his inauguration, Prime Minister Modi vowed to initiate sweeping reforms designed to punish companies that bribe public officials, particularly those involved in infrastructure projects, but he has encountered a political culture resistant to change.

International Cooperation

- Recent years have brought increasing levels of cooperation and coordination between the U.S. and foreign governments. For example in March, U.S., Japanese, Chinese, and Korean authorities began investigating manufacturers of capacitors for cartel activity. These investigations were prompted by a leniency application in the U.S. and other jurisdictions.

- In 2013 the DOJ announced a cooperation program for Swiss banks. About one-third of Swiss banks signed up to participate in the program by the deadline.
- The investigations of the auto-parts industry has brought unprecedented cooperation in international and global enforcement. The DOJ recently credited the Japan Fair Trade Commission for first detecting some of the auto parts conduct at a press conference announcing massive DOJ corporate fines and indictments.
- Assistant Attorney General Leslie Caldwell attributed the success of the DOJ's enforcement actions against a general trading company and a manufacturing company, in connection with alleged bribes they paid to members of the Indonesian Parliament to secure a lucrative power contract, to successful international collaboration.

Today's Panelists

F. Joseph Warin

Partner
Washington, D.C. Office
Tel: 202.887.3609
Fax: 202.530.9608
fwarin@gibsondunn.com

Richard Grime

Partner
Washington, D.C. Office
Tel: 202.955.8219
Fax: 202.530.9652
rgrime@gibsondunn.com

Scott Hammond

Partner
Washington, D.C. Office
Tel: 202.887.3684
Fax: 202.530.9582
shammond@gibsondunn.com

Lori Zyskowski

Partner
New York, N.Y. Office
Tel: 212.351.2309
Fax: 212.351.6309
lzyskowski@gibsondunn.com

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