GIBSON DUNN

Challenges in Compliance and Corporate Governance

January 23, 2020

Panelists:

F. Joseph Warin
Stuart F. Delery
Adam M. Smith
Zainab Ahmad
Michelle Kirschner
Lori Zyskowski

MCLE Certificate Information

MCLE Certificate Information

- Most participants should anticipate receiving their certificate of attendance in four weeks following the webcast.
- All questions regarding MCLE information should be directed to Victoria Chan at (650) 849-5378 or vchan@gibsondunn.com.

Presentation Overview

1

2019:
The Highlights

2

Global
Enforcement &
Regulatory
Developments

3

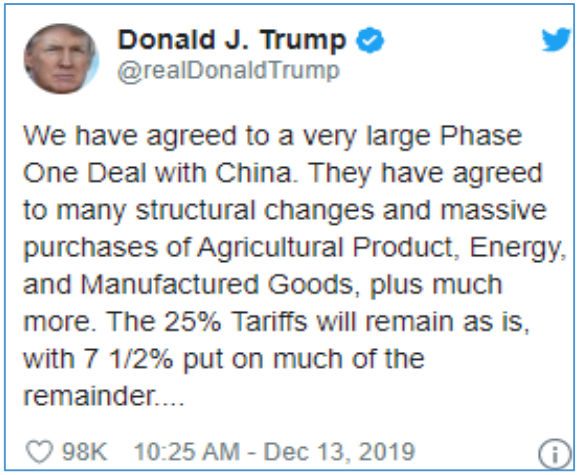
Strategies for
Effective
Compliance

GIBSON DUNN

2019: The Highlights

Shifting Transnational Alliances

- Following the December 20, 2019 approval of the current UK Brexit plan by the British Parliament, and pending approval of the plan by the European Parliament, the UK will formally leave the European Union on January 31, 2020.
  - –Following an 11-month transition period, the UK will begin 2021 with a (likely) very different relationship with Europe.
- Meanwhile, in the United States, Congress approved a revised United States Mexico Canada Agreement ("USMCA"). When ratified by all three parties, the USMCA will replace the 25-year-old North American Free Trade Agreement ("NAFTA").
  - –The United States, Mexico, and Canada signed the deal in November 2018; Mexico ratified it in June 2019, and Canada is expected to ratify it as well.
- In mid-December 2019, the United States and China agreed on a "Phase One" trade deal featuring (1) the Chinese purchase of an unspecified amount of American products and (2) unspecified "structural changes." President Trump signed the deal on January 15, 2020.



Continuing Cross-Border Cooperation

- Increasing globalization has resulted in expanded efforts by regulators to work with foreign counterparts to identify and address misconduct.
- Greater international cooperation also has been hailed as a tool to facilitate DOJ's "anti-piling on" policy, announced in May 2018.
- DOJ has continued to emphasize the significance of the U.S. Clarifying Lawful Overseas Use of Data Act (the "CLOUD" Act) to facilitate the prosecution of crime with transnational elements, described by DOJ as "a model for international cooperation."
  - In October 2019, the United States entered into its first bilateral CLOUD Act Agreement with the UK.

". . . [W]orking cooperatively and efficiently with our foreign counterparts is an absolute necessity for effective law enforcement today."

– Richard W. Downing, Acting Deputy Assistant Attorney General, Principal Deputy Chief, Computer Crime and Intellectual Property Section, Apr. 5, 2019

"Developing . . . close mutual understanding and cooperation is the future. . . . We are not going to catch [criminals operating across borders] unless we can find appropriate ways to work together."

– Lisa Osofsky, SFO Director, Apr. 3, 2019

The CLOUD Act authorizes the U.S. to enter into bilateral executive agreements to facilitate direct law enforcement access to electronic evidence, wherever it is stored.

Converging Approaches to Compliance

- Regulators are applying lessons from the enforcement of different regimes, resulting in more consistent and uniform compliance expectations.
  - DOJ's National Security Division voluntary disclosure guidance mirrors DOJ's Criminal Division policy.
  - Prosecutors in the UK negotiating DPAs have incorporated the U.S. approach in determining what constitutes appropriate compliance and remediation.

> *". . . [I]t is not in the Criminal Division's interest to be opaque about the factors we want our prosecutors to consider when evaluating corporate compliance programs. We want the corporate community to invest heavily in compliance, and do so efficiently and effectively . . ."*
>
> – Brian A. Benczkowski,
> Assistant Attorney General,
> Dec. 4, 2019

- This trend reflects growing agreement on the core elements of an effective compliance program.
- This move towards standardization promises significant benefits for companies, which now will be better able to assess regulators' expectations, identify their obligations, and tailor their compliance programs.

GIBSON DUNN

Global Enforcement and Regulatory Developments

Global Enforcement and Regulatory Developments

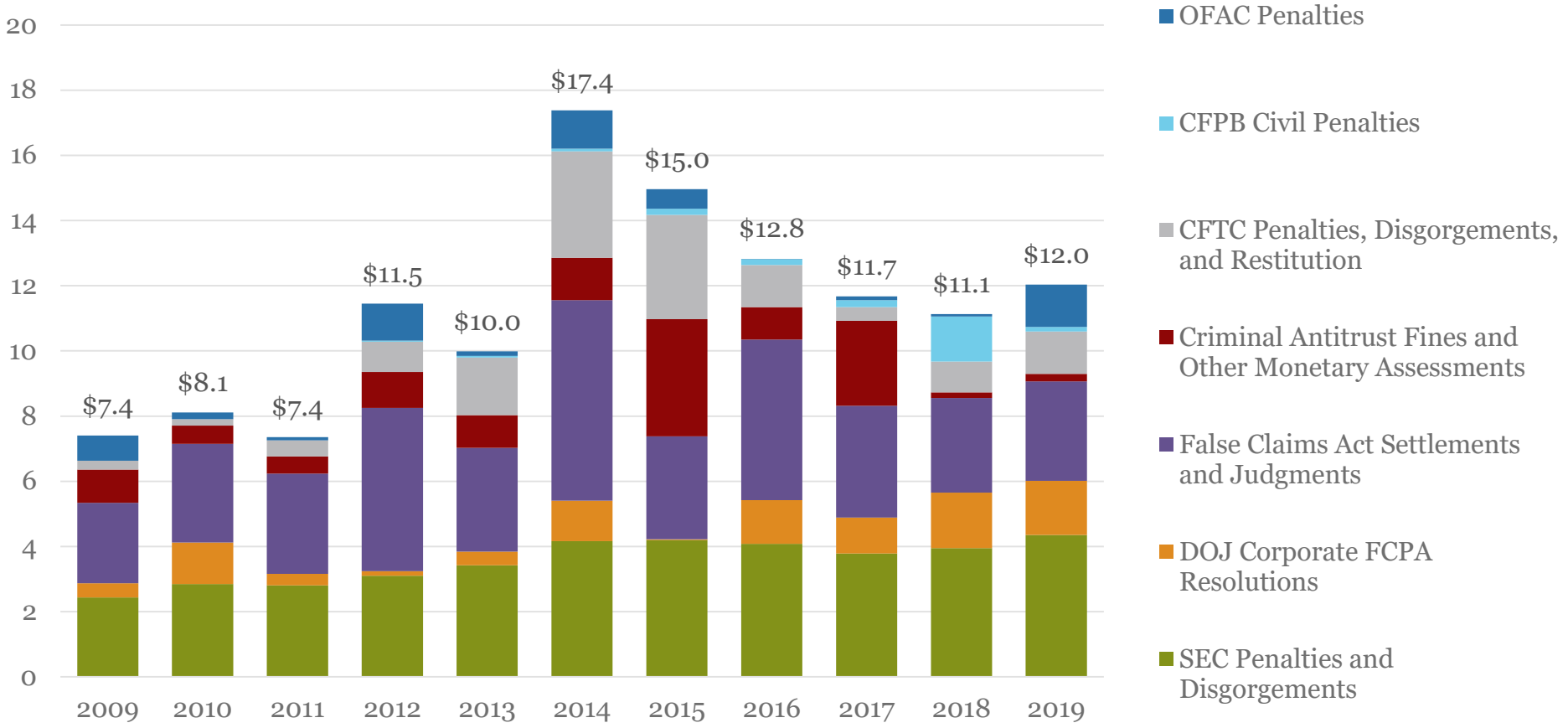
- U.S. Agencies: Priorities, Policies, and Penalties
- Sanctions
- Cyber Risks, Data Privacy, and Cybersecurity
- Foreign Investment in the United States
- BSA/AML
- Corporate Governance Issues
- White Collar and Securities Fraud
- Antitrust
- False Claims Act
- Criminal Tax and Cross-Border Concerns

GIBSON DUNN

U.S. Agencies: Priorities, Policies, and Penalties

U.S. Fines Increase, Driven by OFAC Penalties

Fines, Penalties, and Remedies (In Billions)*



* GDC Internal Aggregations. CFPB Civil Penalties do not include CFPB recoveries and restitutions. The CFPB formally began operating in July 2011. All figures are tracked by fiscal year except for DOJ Corporate FCPA resolutions and OFAC penalties, which are tracked by calendar year.

Top 2019 Fines, Penalties, Disgorgement, & Forfeiture

Anti-Corruption, Antitrust, FCA, FIRREA, and Sanctions Offenses

Amount	Industry/Company	Area
$1.4B	Pharmaceuticals	FCA (DOJ, States/Territories), FTC
$1.3B	Financial Services	Sanctions (OFAC, DOJ, FRB, NY DFS, DANY)
$1.1B	Financial Services	Sanctions (OFAC, DOJ, FRB, NY DFS, DANY, UK FCA)
$1.04B	Telecommunications	FCPA (DOJ, SEC)
$850M	Telecommunications	FCPA (DOJ, SEC)
$300M	Mortgage Origination and Lending	FCA and FIRREA
$296M	Oil & Gas Services	FCPA (DOJ, SEC, and Brazilian Authorities)
$282.7M	Consumer Retail	FCPA (DOJ, SEC)
$275M	Consumer Credit Reporting	Consumer Protection (FTC, CFPB, State/Territorial AGs)
$231.7M	Medical Services	FCPA (DOJ, SEC)
$195M	Pharmaceuticals	FCA
$112.5M	Research University	FCA
$100M	Food Processing Company	Criminal Antitrust

GIBSON DUNN

Department of Justice

DOJ Enforcement in 2019

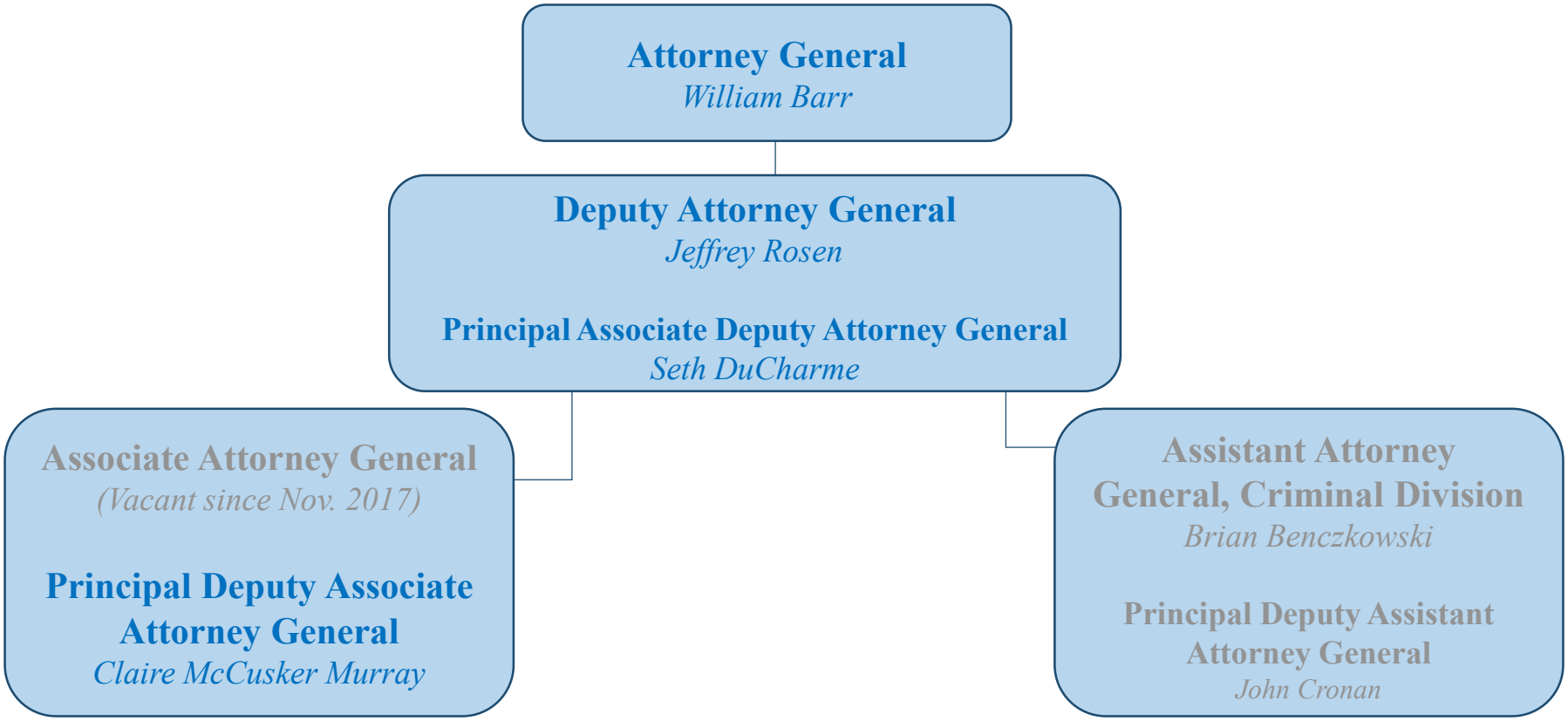
Key Developments

- Attorney General William Barr was sworn in on February 14, 2019.
- Deputy Attorney General Jeffrey Rosen was sworn in on May 22, 2019.
- DOJ 2019 policy announcements included:
  - –Updated guidance from the Criminal Division on the assessment of corporate compliance programs;
  - –Formal guidance from the Civil Division on awarding credit to defendants cooperating with False Claims Act investigations;
  - –Announcement by the Antitrust Division of the creation of a strike force to combat antitrust misconduct in government procurement; and
  - –Updated guidance by the National Security Division on voluntary self-disclosures.
- DOJ continues to coordinate closely with other federal, state, and international agencies to investigate and resolve transnational matters.

DOJ Enforcement in 2019

Changes in Top Leadership

- A number of high-level appointees joined the Department in 2019.



DOJ Enforcement in 2019

Criminal Division Guidance on Evaluating Corporate Compliance Programs

- Evaluation structured around three "fundamental questions" from the Justice Manual:
  1. Is the corporation's compliance program well designed?
  2. Is the program being applied earnestly and in good faith? In other words, is the program being implemented effectively?
  3. Does the corporation's compliance program work in practice?
- The guidance groups twelve compliance topics and sample questions that DOJ considers relevant to compliance program evaluations, including policies and procedures; training; reporting mechanisms and investigations; third-party due diligence; tone at the top; compliance independence and resources; incentives and disciplinary measures; and periodic testing and review.

"[The Evaluation of Compliance Programs] guidance underscores the importance we have long placed on companies employing risk-based, fit-for-purpose compliance programs . . . [the guidance] details the features of effective implementation—from commitment by senior and middle management to incentives and disciplinary measures."

– Brian Benczkowski, Assistant Attorney General, Criminal Division, Oct. 8, 2019

GIBSON DUNN

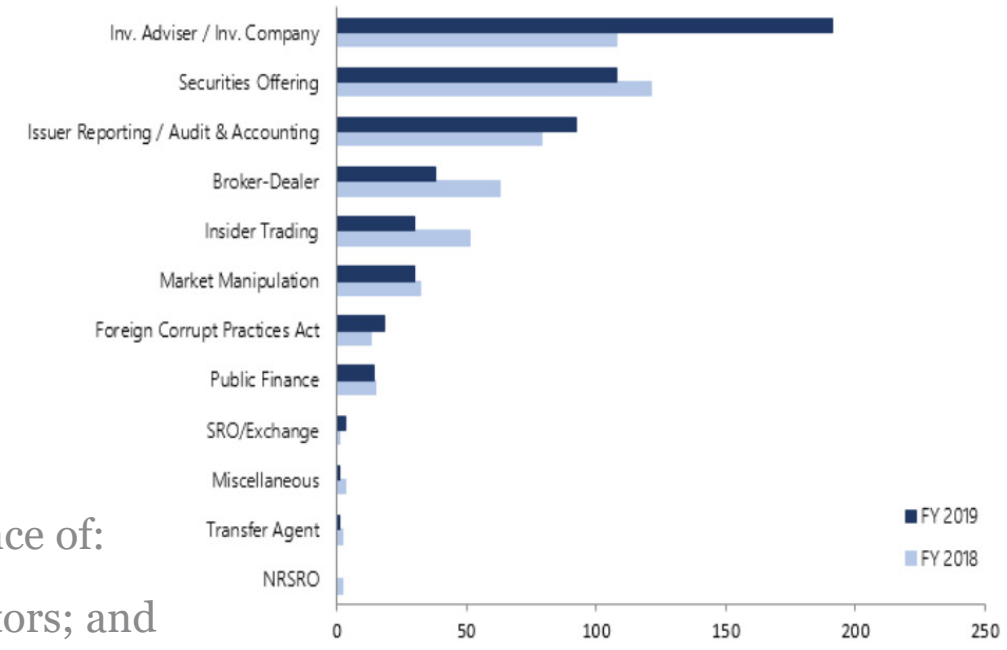
Securities and Exchange Commission

SEC Enforcement in 2019

Review of Key Focus Areas

- The Division of Enforcement's 2019 Annual Report addresses the U.S. Securities and Exchange Commission's ("SEC") efforts with respect to five core principles:
  1. Focusing on the retail investor;
  2. Focusing on individual accountability;
  3. Keeping pace with technological change;
  4. Imposing remedies that most effectively further enforcement goals; and
  5. Constantly assessing the allocation of resources.
- In particular, the report stresses the importance of:
  - –Preventing misconduct against retail investors; and
  - –Preventing cyber-related misconduct.

Types of Cases (SEC Standalone Actions)



SEC Division of Enforcement 2019 Annual Report

SEC Enforcement in 2019

Key Developments

- The Share Class Selection Disclosure Initiative led to the SEC ordering 79 investment advisers to return more than $125 million to affected investors based on the advisers' failures to disclose conflicts of interest.
- The SEC issued a package of rulemakings and interpretations concerning retail investors and investment advisers. One interpretive release aimed "to reaffirm—and in some cases clarify—certain aspects of the fiduciary duty that an investment adviser owes to its clients." The final guidance, among other things:
  - –Reaffirmed that an adviser's fiduciary duty to its clients may not be waived; and
  - –Clarified that an adviser's fiduciary duty depends substantially on the functions it has agreed to perform.
- Chairman Clayton announced the creation of a Teachers' Initiative and a Military Service Members' Initiative, both designed to focus additional enforcement on behalf of teachers, soldiers, and veterans.

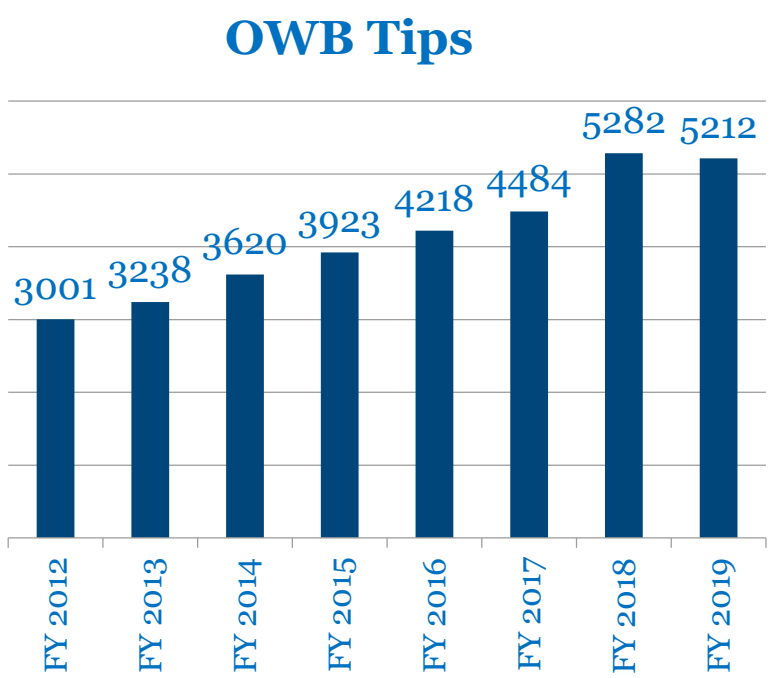
"This rulemaking package was a long time coming . . . These actions will significantly benefit Main Street investors . . . Retail investors also will know that their investment professional, whether an investment adviser or a broker dealer, is prohibited from putting their interests ahead of the retail investor's interests."

– Jay Clayton,
SEC Chairman,
Nov. 14, 2019

SEC Enforcement in 2019

Whistleblower Update

- In FY 2019, the SEC reported a slight decrease from tips received in FY 2018, which had the greatest number of tips on record.
  - –Nearly 300 tips received related to cryptocurrencies.
- In addition to U.S.-based tips (received from every state), the SEC also received tips from individuals in 70 different countries.
- The SEC awarded ~$60 million in whistleblower awards to eight individuals, including $37 million to a single whistleblower. Since the program's inception, the SEC has claimed over $2 billion in monetary sanctions in matters brought with information from whistleblowers, and has awarded ~$387 million to 67 individuals.

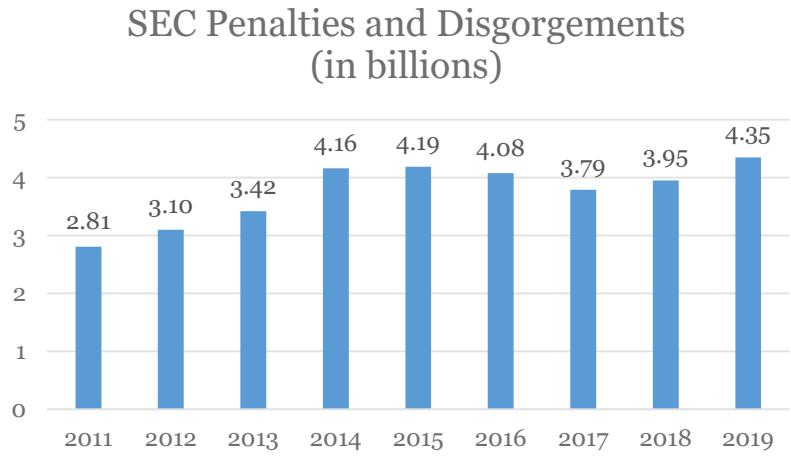


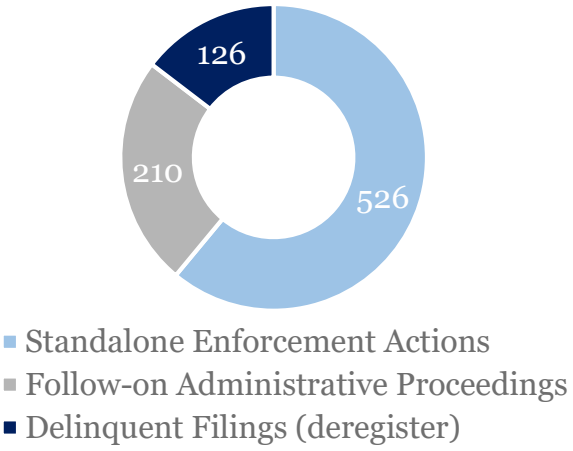
- Amendments proposed by the SEC to its whistleblower program in June 2018 remain under consideration by the Commission, with new rules expected to be adopted in FY 2020. These rules, among other things, would clarify the requirements for anti-retaliation protections under the whistleblower statute following the Supreme Court's ruling in *Digital Realty Trust, Inc. v. Somers* and would provide tools to increase efficiencies in the claims review process.

Details on SEC Enforcement in 2019

Key Cases

- The Supreme Court held in *Lorenzo v. SEC* that the dissemination of false or misleading statements with intent to defraud can come within the scope of SEC Rules 10b-5(a) and (c), even if the person disseminating the information did not "make" the statements under the *Janus* standard.
- The D.C. Circuit held in *Robare v. SEC* that, under Section 207 of the Adviser's Act (addressing disclosures to the SEC), the required "willfulness" standard cannot be established by negligent conduct.
  - –This constitutes a major departure from the SEC's interpretation of the standard since *Wonsover* (2000).
- The Supreme Court granted certiorari in *Liu v. SEC* to consider whether the SEC may seek and obtain disgorgement from a court as "equitable relief" for a securities law violation. Oral arguments are scheduled for March 2020.





PCAOB Update

- FY 2019 marked the first year in which the PCAOB required audit reports for large issuers to feature Critical Audit Matters ("CAMs"), identifying especially challenging aspects of the audit.
  - –CAMs most commonly relate to goodwill and revenue.
  - –SEC and PCAOB scrutiny of CAM disclosures is expected in 2020, as well as post-implementation review.

> *"While we are proud of what we have accomplished so far, much more remains to be done to fulfill our strategic vision."*
>
> – William Duhnke, PCAOB Chairman, Dec. 18, 2019

- The PCAOB focused its 2019 inspections on, among other issues, use of technology, independence, and audit responses to cybersecurity and digital assets.
- The PCAOB initiated a new five-year plan in 2019 to overhaul its quality control rules and streamline its processes for inspecting audit firms.
  - –The Board intends to advance proposals in 2020 for a rule governing audit firms' approaches to quality control and the creation of a permanent program for the inspections of broker-dealers.
- Relatedly, the SEC recently proposed amendments to help modernize its auditor independence rules, and has indicated that it hopes to finalize these in 2020.

GIBSON DUNN

Commodity Futures Trading Commission

Details on CFTC Enforcement in 2019

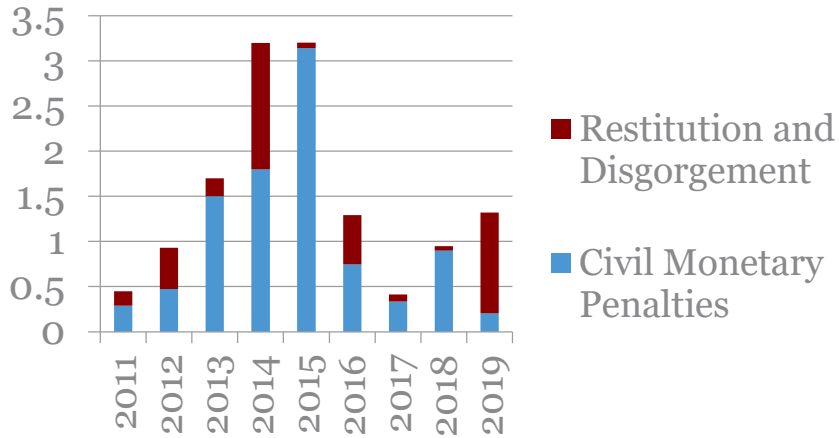
Key Statistics and Trends

- The CFTC's Division of Enforcement filed 69 actions in FY 2019, an increase over the average for the previous five years, and obtained more than $1.3 billion in total monetary relief.
- In publishing its first Enforcement Manual in 2019, the Division of Enforcement signaled an interest in becoming a more active enforcer. Notably, the CFTC increasingly is working in parallel with criminal authorities: in FY 2019, it filed 16 parallel cases, an all-time high.
- As in previous years, the CFTC focused on charges of commodities fraud, manipulative conduct, false reporting, and spoofing. In addition, the CFTC issued an Advisory on Violations of the Commodity Exchange Act Involving Foreign Corrupt Practices, indicating a new interest in investigating and addressing allegations of corruption.

"Combating misconduct that affects our financial markets has truly become a team effort, and that is particularly true with respect to foreign corrupt practices. We at the CFTC will do our job as part of the team to identify this type of misconduct in our markets and hold wrongdoers accountable, working closely with our enforcement partners domestically and abroad."

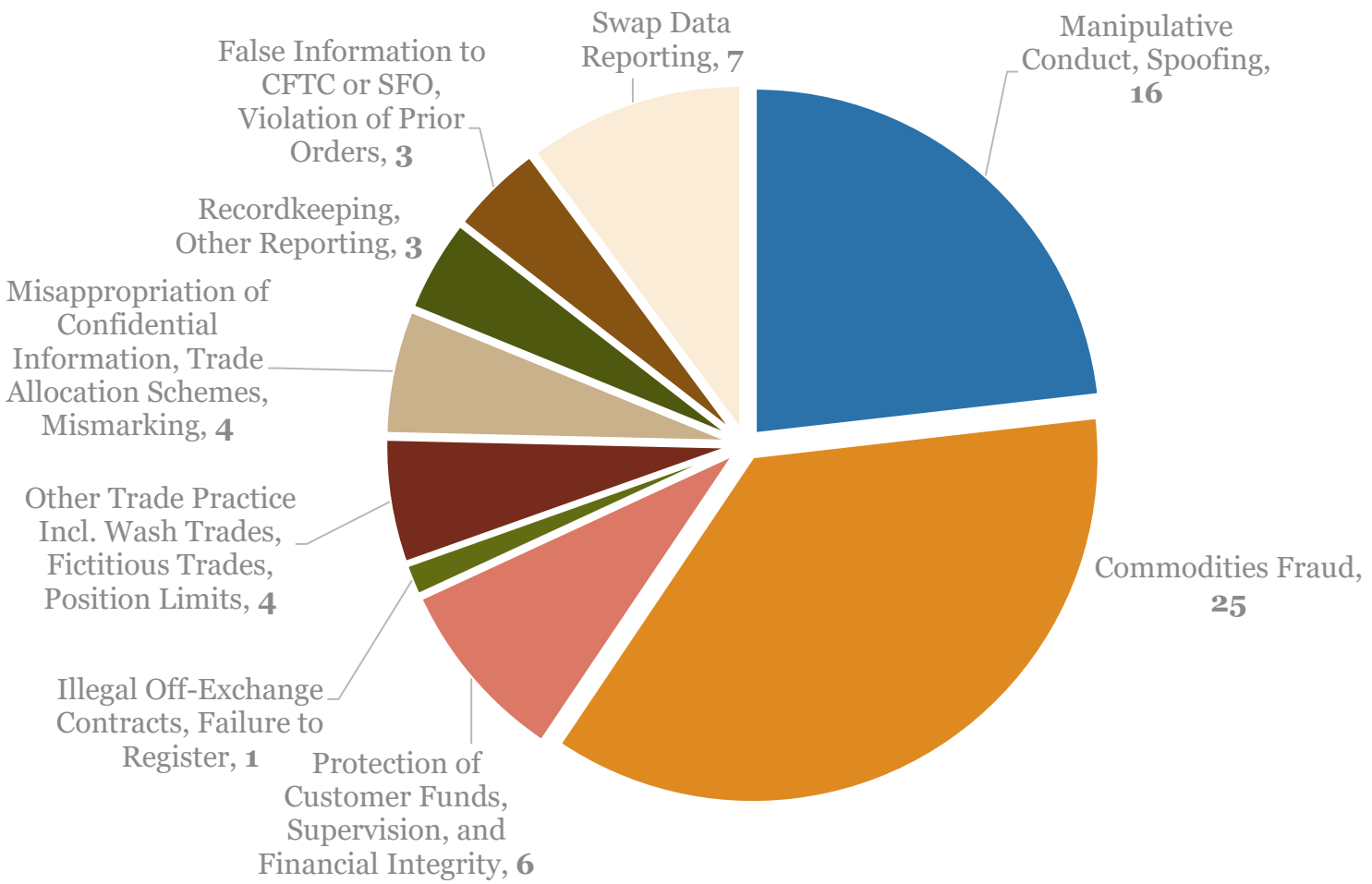
– James McDonald, CFTC Enforcement Director, Mar. 6, 2019

CFTC Recovery (in billions)



Details on CFTC Enforcement in 2019

2019 Enforcement Actions by Category



https://www.cftc.gov/PressRoom/PressReleases/8085-19

Details on CFTC Enforcement in 2019

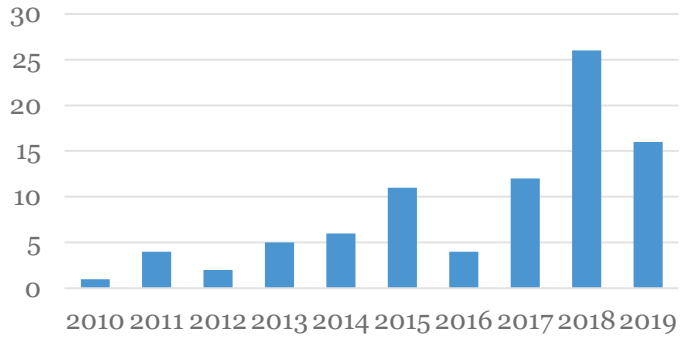
Focus on Spoofing

- The CFTC continued to treat spoofing—i.e., bidding with an intent to cancel before execution of the trade—as a top priority in FY 2019.
- After creating a Spoofing Task Force and filing 26 cases in 2018, in 2019 the CFTC filed 16 enforcement actions—its second-highest total ever—based on manipulative conduct/spoofing.
  - Increased collaboration with federal law enforcement authorities, technological developments, and the proliferation of automated trading systems—including high-frequency trading—appear to play important roles in the spoofing enforcement push.
- The CFTC's spoofing enforcement underscores two of the agency's key themes: (1) cooperation with enforcement counterparts, and (2) individual accountability. For example:
  - In July, and in parallel to a related DOJ prosecution, the CFTC ordered Merrill Lynch Commodities, Inc. to pay ~$25 million for spoofing and manipulation.
  - In September, the CFTC and DOJ announced parallel civil and criminal enforcement actions against three traders allegedly involved in spoofing in precious metals markets.

"If left unchecked, spoofers will gain an unfair and unlawful advantage over others, which hinders competition, undermines market integrity, and harms law-abiding victims. Spoofing drives traders away from our markets [and] harms businesses, large and small, that use our markets to hedge their risks in order to provide stable prices[.]"

– James McDonald, CFTC Enforcement Director, Jan. 29, 2018

CFTC Enforcement Actions Involving Manipulative Conduct or Spoofing



GIBSON DUNN

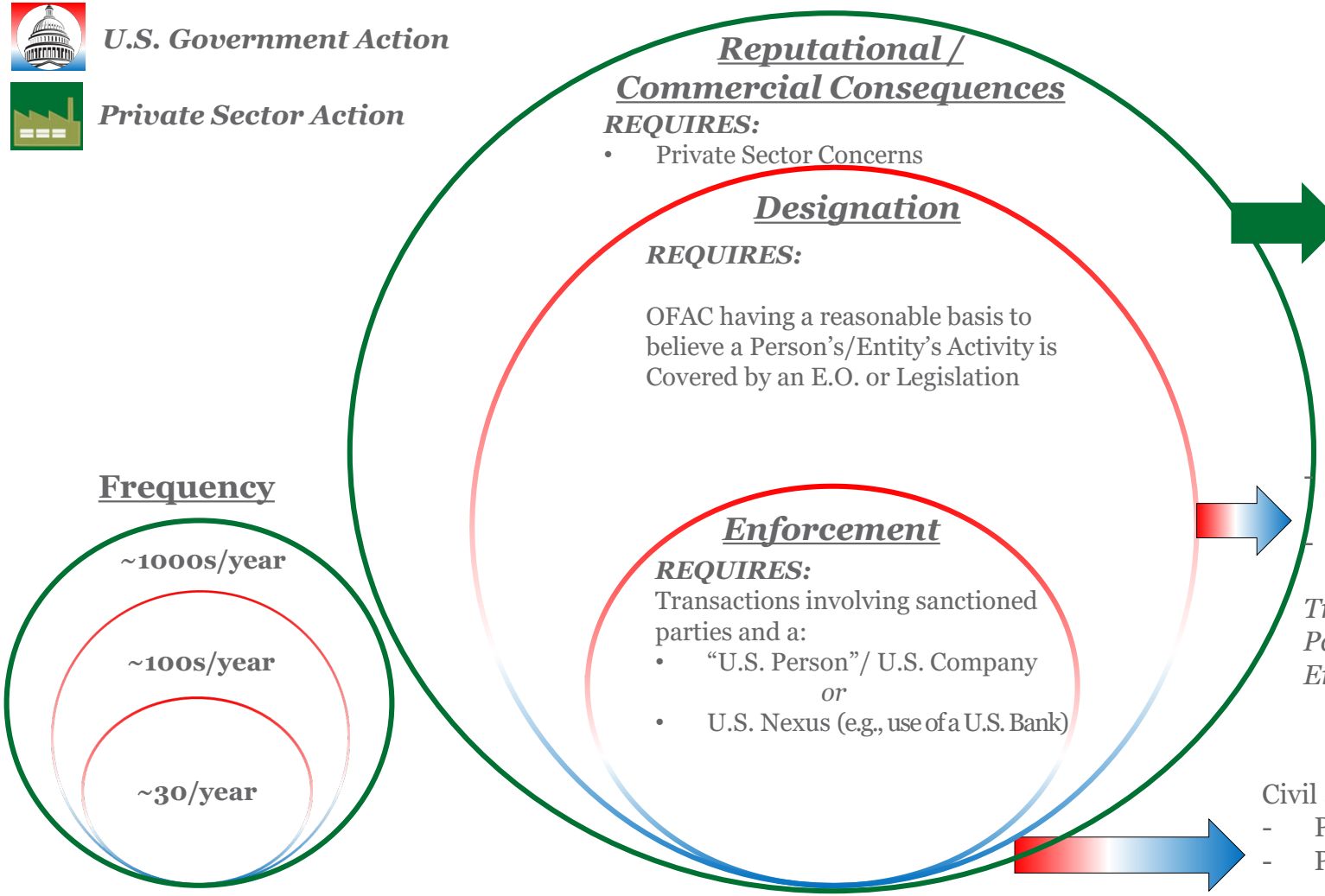
Sanctions

Sanctions

Refresher on Sanctions Risks

U.S. Government Action

Private Sector Action



Possible Outcomes

De-Risking or Limited Transactions

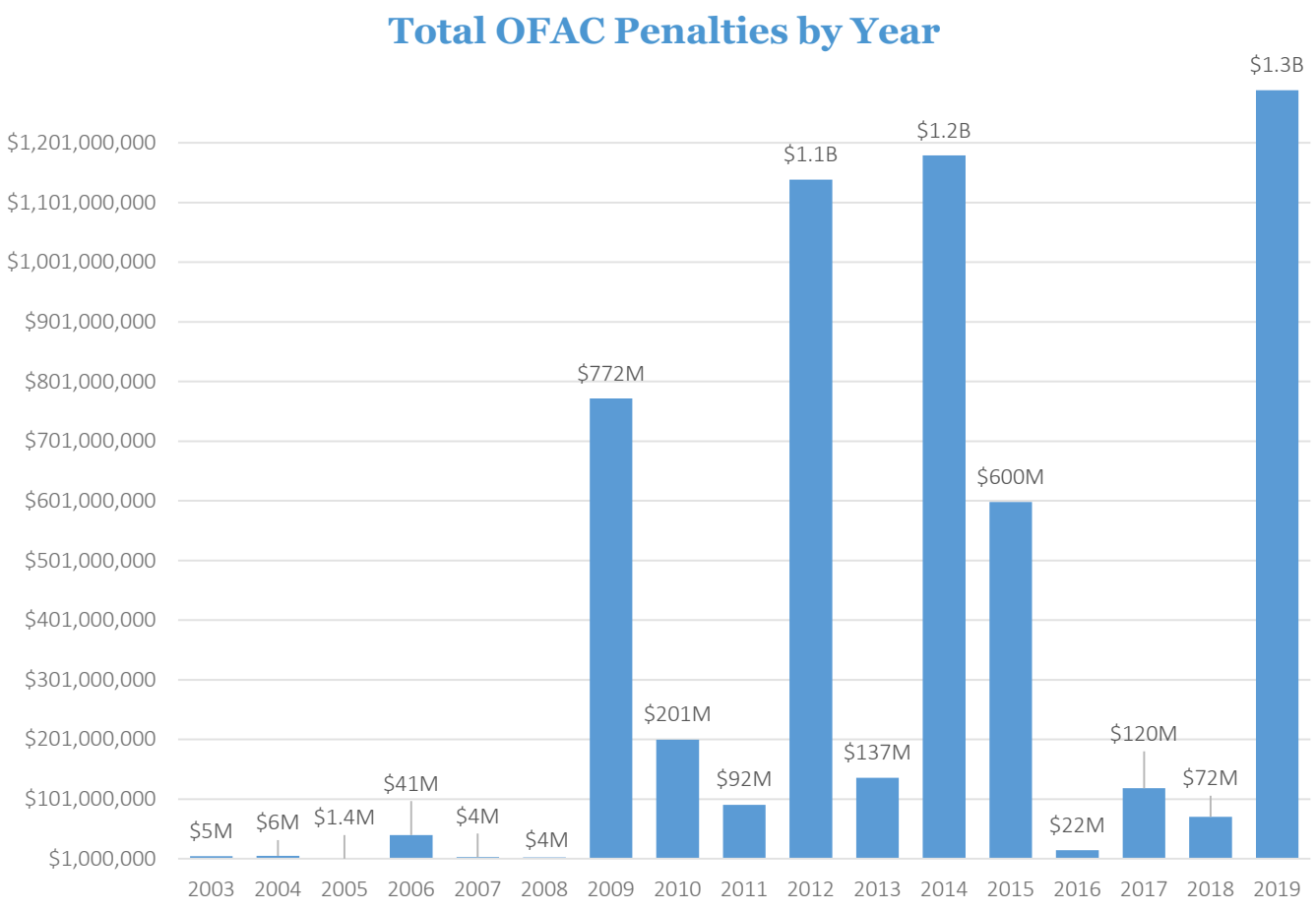
- Appearance on SDN List; or,
- Limiting Access to U.S. System

Transactions with Designated Parties can lead to Enforcement

Civil and Criminal Consequences
- Potential Substantial Fines
- Potential Incarceration

Sanctions

U.S. Update: 2019 By the Numbers



OFAC Penalties

- 2019 was a record year for OFAC enforcement: ~$1.3 billion (largest amount ever) imposed.
- Average penalty in 2019 was nearly $43 million.
- OFAC had 30 enforcement actions in 2019—the most in a decade.
- Statutory amounts for penalties have increased to more than $300,000 or twice the value of the underlying violative transaction.

Sanctions
U.S. Update: 2019 Enforcement Developments and Trends

- **Enforcement Credits**: OFAC announced that it will drastically narrow the credit given by the Treasury Department to fines paid to other agencies as part of joint settlements, limiting credits to only those addressing the same conduct.
- **Implementation of Compliance Certifications**: OFAC has established a go-forward requirement that settlement agreements with OFAC will require companies to sign on to binding future-looking compliance commitments.

> C. **Compliance Commitments:** Respondent has terminated the conduct described above and has established, and agrees to maintain, sanctions compliance measures that are designed to minimize the risk of recurrence of similar conduct in the future. Specifically, OFAC and Respondent understand that the following compliance commitments have been made:

[Acteon (Mar. 29, 2019)]

- **Courts Weigh In***:* On December 31, 2019, the U.S. District Court for the Northern District of Texas found that a penalty imposed by OFAC on Exxon violated the Fifth Amendment's Due Process Clause.

Sanctions

U.S. Update: 2019 Enforcement Developments and Trends

Focus on Non-Bank Enforcement . . .

- In recent years, OFAC—once known principally for its financial-sector enforcement—has become equally aggressive in non-bank enforcement.
- 2019 has seen the enforcement of a diverse sanctions program with a focus on co-mingling/supply chain due diligence, successor liability, and individual liability.
- Examples include actions against:
  - –ELF – the company's compliance program and its supplier audits failed to discover that approximately 80% of false eyelash kits supplied by two of its China-based suppliers contained materials from the DPRK;
  - –Acteon – successor liability assessed for the first time against financial owners, not operators, in the private equity space; and
  - –KollMorgen – OFAC sanctioned a senior company official in addition to the corporate enforcement action.

Sanctions

U.S. Update: 2019 Enforcement Developments and Trends

. . . and Continued Big-Bank Enforcement

- Massive enforcement actions by OFAC against Standard Chartered ($657,040,033 penalty for violations of Burma, Cuba, Iran, Sudan, and Syria sanctions) and UniCredit ($611,023,421 penalty for violations of Burma, Cuba, Sudan, Syria, WMD, Libya, and terrorism sanctions).
  - Both cases are legacy matters. Penalties resulted from activities that occurred more than a decade ago for both banks.
- These cases indicate OFAC's:
  - Willingness to enforce against parties for longstanding, historic activities;
  - Increasing reliance on tolling agreements (to avoid statute of limitations issues); and
  - Bold action in imposing enormous fines.

Together, these trends counsel heightened consideration concerning voluntary self-disclosure to OFAC of potential sanctions violations.

Sanctions

U.S. Update: NSD Updated Guidance on Voluntary Self-Disclosure

- On December 13, DOJ's National Security Division ("NSD") announced changes to its 2016 policy governing the treatment of voluntary self-disclosures ("VSD") in criminal sanctions and export control investigations. Highlights of the NSD VSD guidance include that:
  - DOJ now has made the policy applicable to financial institutions (previously excluded from the policy);
  - In the absence of aggravating factors, a company that voluntarily discloses to DOJ and satisfies the other requirements set out in the policy presumptively will resolve through a Non-Prosecution Agreement ("NPA") with no fine assessed;
  - Where aggravating circumstances warrant an enforcement action beyond an NPA, companies that otherwise satisfy the VSD requirements will be eligible for an at least 50% reduction off the statutory base penalty (effectively capping the penalty at the dollar value of the violative transaction) and DOJ will not require a monitor if the company has implemented an effective compliance program; and
  - Successor companies that identify a violation by a merged or acquired entity through timely due diligence and voluntarily self-disclosure also will be entitled to a presumption of an NPA.
- In many respects, the updated NSD VSD guidance brings the VSD calculus closer to that employed by companies determining whether to voluntarily disclose potential FCPA violations.

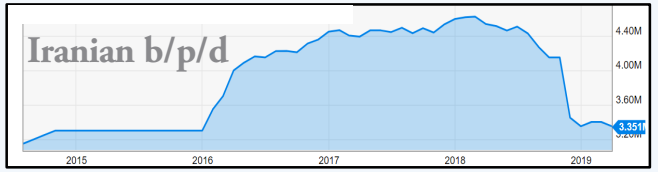
Iran Sanctions Program

Key Developments

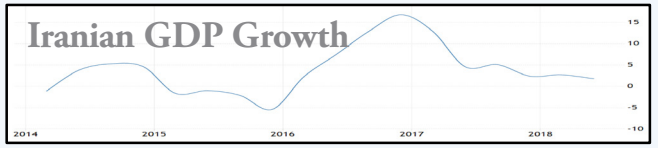
- Following the May 2018 announcement by President Trump that the United States would withdraw from the Nuclear Deal, in November 2018 almost all sanctions were reinstated—i.e., hundreds of entities returned to the sanctions list, many with secondary sanctions implications.
- In May 2019, the U.S. eliminated waivers allowing the purchase of oil by "significant reducers."
- 2020 has seen new sanctions, substantial enforcement actions, and harsh rhetoric between Washington and Tehran.
  - In January 2020, the White House announced new sanctions against Iran in the wake of Iran's missile strike on a U.S. base in Iraq.
- Although Europe and Japan have tried to save the Nuclear Deal (e.g., via Europe's "non-USD" trading system, which has had limited takers), Iran has exceeded limits on enrichment. Europe now has formally accused Iran of breaking the Nuclear Deal, and in mid-January triggered the Deal's dispute mechanism.

The Impact

- Iranian oil production has plummeted



- Iranian economy under increasing pressure



- Tehran forced to provide discounts and look for alternate sales, leading to Grace 1
- Sanctions evasions tactics and violence in the Straits of Hormuz have expanded

Russia Sanctions Program

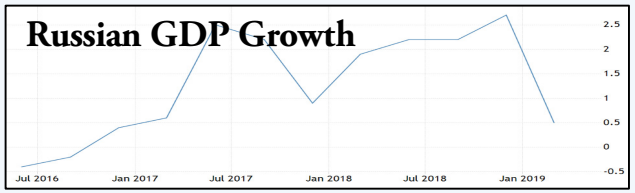
Key Developments

- U.S. and EU sanctions against Russia have continued since 2014, with increasing concern about Russian election interference following the EU Parliamentary elections and in light of the upcoming 2020 U.S. presidential contest.
  - –U.S./EU unity is being tested on Nord Stream 2.
- Legislation has been proposed in the United States that could significantly enhance sanctions against Russian energy majors if interference is found after 2020. In the meantime, some likely legislation will ramp up sanctions pressure on Russia focusing on the country's energy and defense sectors.
- Third-party countries are being collaterally implicated due to secondary sanctions.

The Impact

- Russian oil production has been stable—but projects abroad have been impacted due to expanded Directive 4

- Russian economic growth has been weak



- The United States recently imposed its first enforcement fine for violations of its Russia sanctions. Meanwhile, numerous lawsuits have been lodged in the United States by sanctioned Russian oligarchs, and a longstanding Russian counter-sanctions proposal is being considered once again in the Duma.

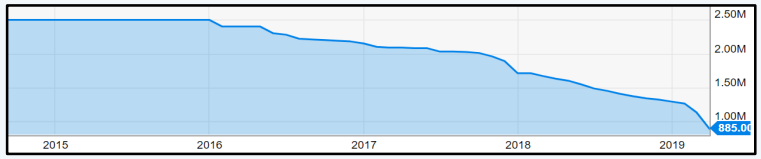
Venezuela Sanctions Program

Key Developments

- The United States sanctioned PdVSA, the Venezuelan state-owned oil company, in January 2019. The impact of the sanction has been felt on numerous MNCs and oil services firms working in Venezuela and/or providing petroleum products globally.
- Sanctions recently have been enhanced to focus on "diluents" and designating parties who provide "material support" to Venezuela's oil sector and/or who provide Venezuelan products to other states.

The Impact

- Venezuelan oil production continues to decline



- Venezuela's economy continues its tailspin—2019 GDP was projected to decline 25%.

- Maduro's regime has become more aggressive, particularly following the April 2019 uprising—shutting down opposition, attempting sanctions evasion, and leaning on weaker neighbors in the Caribbean. After certain Maduro allies attempted to block Guaidó's reelection as president of the National Assembly, the United States announced new sanctions as part of a "maximum pressure" campaign against Maduro.
- Growing similarities are apparent in evasion techniques utilized by sanctioned jurisdictions, including Venezuela, Iran, and North Korea—AIS shutoffs, ship-to-ship transfers, etc.
- Increasing sanctions pressure is likely in the run-up to the 2020 U.S. elections, due to the importance of the Florida vote.

Sanctions

Now What? Sanctions Compliance Best Practices

- In May 2019, OFAC published "A Framework for OFAC Compliance Commitments," which sets out for the first time the agency's views on the essential components of an effective sanctions compliance program. These include:
  - –Management commitment;
  - –Risk assessment;
  - –Internal controls;
  - –Testing and auditing; and
  - –Training.

> *"Most U.S. and non-U.S. companies that engage in international trade have practices that fall short of the elements described in the framework."*
>
> – Andrea Gacki,
> OFAC Director,
> June 13, 2019

- Companies should treat the new guidance as setting baseline expectations for their sanctions compliance policies and procedures.
- OFAC will consider whether all of the components above are present in a company's compliance program in determining any findings of violations and resulting imposition of monetary penalties.

Sanctions

UK & European 2019 Developments

Europe

- The EU continued to expand existing sanctions and implement new ones. In May, it established a sanctions framework for targeted restrictive measures to deter and respond to cyber-attacks that constitute an external threat to the EU or its Member States.
- The Blocking Statute puts EU Operators in a bind: risk OFAC enforcement or action by European authorities.

> *"To support our economic sovereignty, I want [the European Commission] to develop proposals to ensure Europe is more resilient to extraterritorial sanctions by third countries…"*
>
> – Ursula von der Leyen, President of the European Commission, Sept. 10, 2019

UK

- The UK government is preparing to introduce a new targeted sanctions regime immediately after Brexit, which will enable the UK to freeze the assets of foreign citizens deemed responsible for human rights abuses (a.k.a. "Magnitsky" style sanctions).
- The Office of Financial Sanctions Implementation ("OFSI") issued its largest fine – £146,341 (~$190,000) to a telecommunications provider, Telia Carrier UK Limited, for breach of the EU's Syria sanctions. OFSI originally imposed a fine of £300,000 (~$390,000), but this was reduced by the responsible Government Minister.

Sanctions

Now What? Sanctions Compliance Best Practices

Appropriate due diligence policies and procedures by gatekeepers and promotion of beneficial ownership transparency for legal entities.

Any indication that documentation has been manipulated should be considered a red flag and should be investigated prior to transacting.

Research companies, individuals, and entities involved in the transactions.

Parties to transactions may be subject to different sanctions depending on the parties and jurisdictions, so clear communication is critical.

Internal and external resources, including sanctions databases, can be leveraged as essential aspects of an effective compliance program.

Sanctions

Now What? What May Be Next

- Key issues to consider as we move into a new decade of sanctions enforcement and compliance include the following potential developments:

Enhanced Expectations for Export Controls Compliance
- Increase in export-related restrictions may lead to the need for additional screening for export control issues and consequent new sector-wide requirements.

Imposition by OFAC of Compliance Monitors
- OFAC's new compliance approach increases work for the regulated community and the agency. OFAC remains small (~200 staff) and likely lacks resources for the new oversight requirements. OFAC could follow other agencies and address resource issues via the use of compliance monitors.

UK Sanctions Post-Brexit
- How will London deal with sanctions after it leaves the EU? In the short term, London will adopt the EU's existing measures, but its approach over the longer term is uncertain.

Counter-Sanctions to U.S. Measures
- Pending queries remain over how and if the EU will enforce sanctions against U.S. unilateral measures; whether China will develop its own "black list" to respond to Huawei restrictions; and whether Russia's counter-sanctions will be approved by the Duma.

U.S. 2020 Elections
- Sanctions could become even more politicized, but there will likely be more measures and stronger enforcement in the lead-up to 2020 across the full range of sanctions programs.

GIBSON DUNN

Cyber Risks, Data Privacy, and Cybersecurity

Focus on Cybersecurity

Data Security, Digital Currencies, and Sanctions

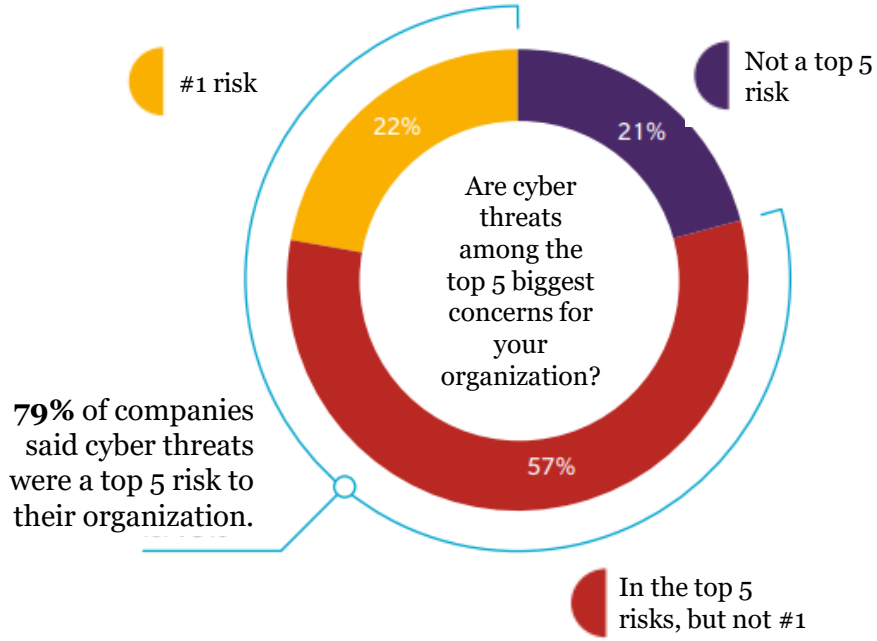
- Increasing digitization poses significant challenges to regulators and companies alike. These include:
  - –Attempts by regulators to apply analog rules to digital currency, which operates as an alternative to the traditional financial system;
    - For example, OFAC must consider blocking digital assets to maintain the efficacy of the sanctions system.
      - ➢The agency recently has started listing digital wallet addresses.
      - ➢President Trump has signed an executive order prohibiting transactions in the Venezuelan government's cryptocurrency, the Petro.
  - –Addressing the inherent instability of cryptocurrency, which lacks the infrastructure, predictability, reliability, and protections of dollar-based international trade; and
    - Litigation continues following the presumed death of Quadriga founder with sole access to as much as $190 million in investor funds.
  - –Harmonizing cyber risks with cyber defenses.
    - Data obtained in cyber attacks may be used to successfully empty targeted bank accounts.

Cyber Risks, Data Privacy, and Security

Considerations for Executives and the Board

- Surveyed directors of public companies named "changing cybersecurity threats" as one of the top five trends predicted to impact their companies in 2020.[1]
- 51% of organizations reported that they did not believe they were ready for a cyber attack or breach event, based on a survey of 800 senior executives worldwide.[2]
- In the event of a cyber attack, companies can face demands from various regulators who want a seat at the table in any resolution, such as the NYDFS, SEC, and CFTC for financial entities, in addition to more traditional cybersecurity regulators like the FTC.
- Cyber attacks can put companies in the position of being a victim and a defendant in potential civil litigation and regulatory enforcement matters.

Companies View Cyber Threats as a Top Priority



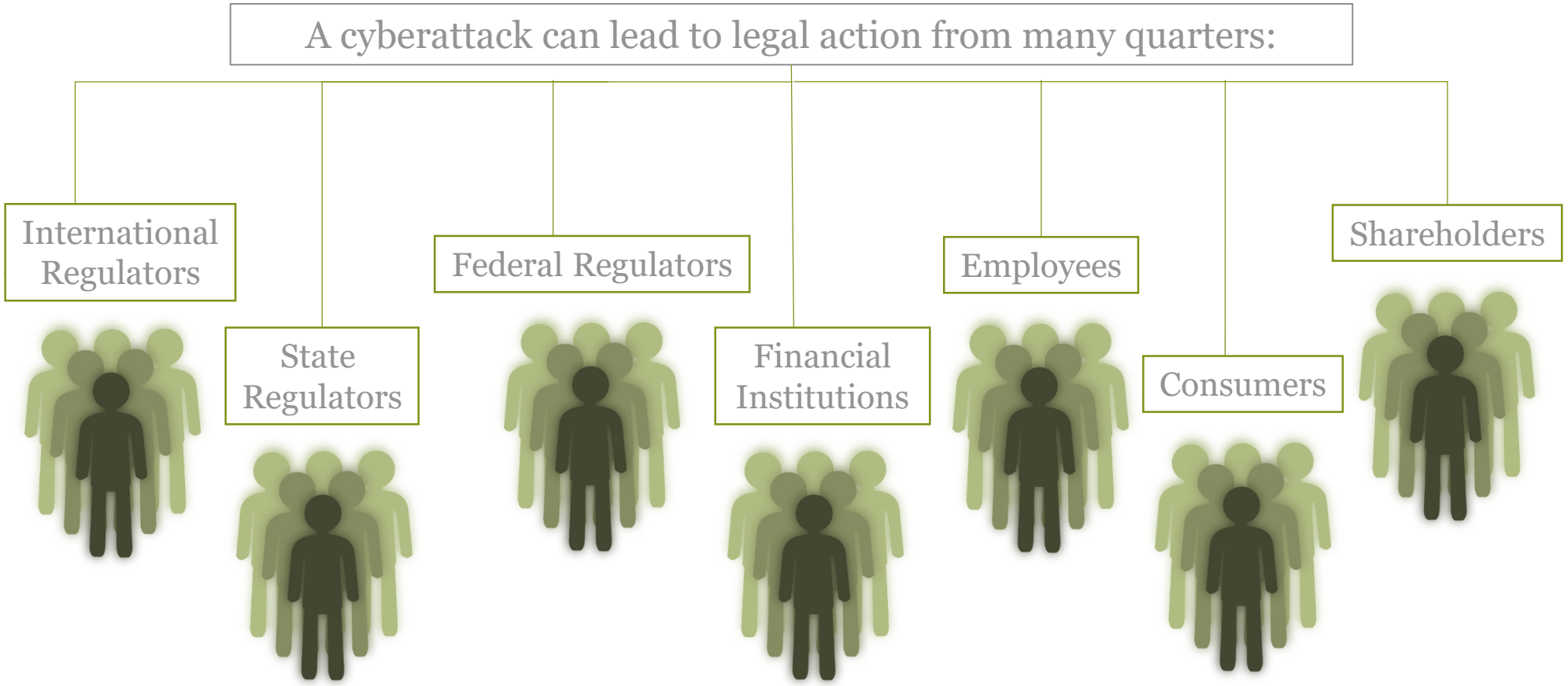
79% of companies said cyber threats were a top 5 risk to their organization.

Source: Marsh and Microsoft Global Cyber Risk Perception Survey, September 2019

1 Nat'l Assoc. of Corporate Directors & Partners, *2020 Governance Outlook*
2 FireEye Cyber Trendscape Report, July 2019

Focus on Cybersecurity

Pervasive Breach-Related Risk

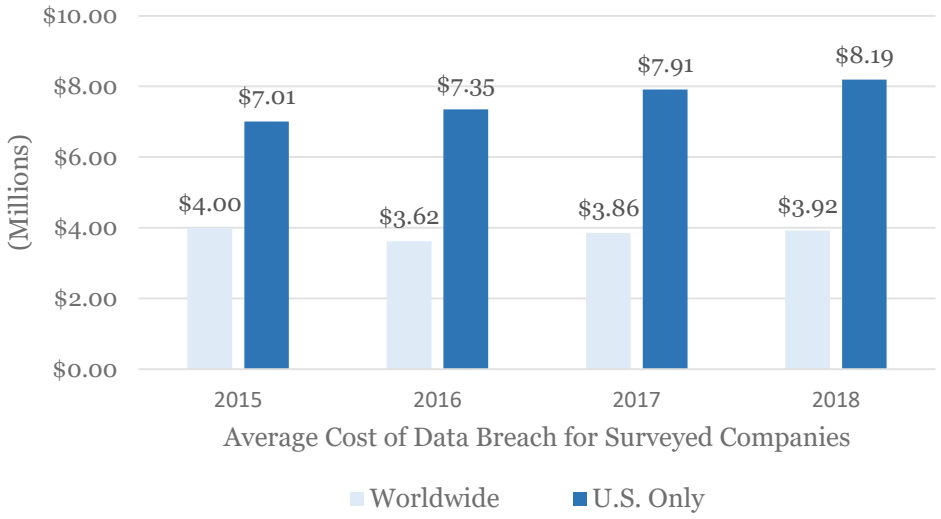


Cyber Risks, Data Privacy, and Security

Threats and Trends

- Malicious or criminal attacks (rather than human error or system glitches) continue to rise as a cause of data breaches.
  - Malicious attacks led to 51% of total data breaches between July 2018 and April 2019, versus 48% and 47% in prior years.
  - Malicious attacks are the costliest type of data breach on average.
- Aside from the direct costs of cyber incidents, failure to timely or comprehensively disclose material cyber risks or incidents can lead to subsequent enforcement actions.
- Increasingly sophisticated ransomware remains an area of concern.
  - For example, the city of New Orleans declared a state of emergency in December 2019 due to a ransomware attack.
- Regulators emphasized in 2019 that cybersecurity risk management must include security assessments of third-party vendors with access to internal corporate networks.

Average Cost of Data Breach Increased 16.8% in the United States from 2015 to 2018



Data compiled from Ponemon Institute – 2019 Cost of Data Breach Study and Ponemon Institute – 2018 Cost of Data Breach Study and Ponemon Institute – 2017 Cost of Data Breach Study and Ponemon Institute – 2016 Cost of Data Breach Study

Cyber Risks, Data Privacy, and Security

Litigation and Enforcement Developments

- Companies continue to enter into significant monetary settlements in lawsuits related to data breaches (derivative suits, securities class actions, and consumer class actions). Equifax, whose 2017 data breach exposed Social Security and other personal data for nearly 150 million people, is illustrative:
  - Equifax agreed to pay up to $700 million to settle multi-district consumer class action litigation based on the breach, with up to $425 million to be set aside directly for consumers.
    - Equifax agreed to pay $100 million to the CFPB in civil penalties, and $175 million to 48 states, the District of Columbia, and Puerto Rico.
    - The FTC did not fine Equifax due to its limited authority to impose civil penalties for first-time offenses—prompting the agency to call on Congress to pass a law allowing it to do so in the future.
    - Equifax will also be required to spend "a minimum of $1 billion for data security and related technology over five years."

  - A putative class against current and former corporate officers at Equifax, originally filed in 2017, continues in the Northern District of Georgia.
  - This litigation follows a 2018 non-monetary settlement whereby Equifax agreed to enter into a consent order with eight state regulatory agencies and take corrective action to improve its cybersecurity defenses.
- A district court in July 2019 approved Yahoo!'s $117.5 million resolution to settle multi-district litigation concerning several alleged data breaches and security issues from 2012 to 2016. Earlier, in January 2019, a district court accepted a $29 million resolution by former Yahoo! officers and directors to settle a consolidated derivative lawsuit—likely the first case where shareholders received monetary damages in a derivative lawsuit relating to an alleged data breach.

Cyber Risks, Data Privacy, and Security

Regulatory Developments: SEC

- Cybersecurity remains a priority for the SEC: the Division of Enforcement continued to list cyber-related misconduct as a focus, and the Office of Compliance Inspections and Examinations ("OCIE") listed cybersecurity as an examination priority.
- Two FY 2019 SEC enforcement actions alleged violations of Regulation Systems Compliance and Integrity ("Reg SCI"), an SEC rule aimed at securing markets' technological infrastructure.
  - The settlement of a Reg SCI action against a clearing agency, Options Clearing Corp., required the company to create a new board committee focused on regulatory compliance operating separately from the Audit Committee.
- OCIE published a list of common compliance issues for broker-dealers and investment advisers related to privacy notices and safeguarding policies (Regulation S-P).
  - Issues included failure to provide privacy and opt-out notices to customers; to have written policies on safeguarding information; and to properly implement polices to safeguard customer information.
- The SEC also increased enforcement related to digital assets and initial coin offerings, with 21 enforcement actions in FY 2019 (up from 13 in FY 2018 and three in FY 2017).

Cyber Risks, Data Privacy, and Security

Regulatory Developments: FTC

- The FTC continued pursuing cybersecurity and data protection enforcement in FY 2019, with settlements that included what it characterized as "strong injunctive provisions . . . that go beyond requirements from previous data security orders."
- FY 2019 saw seven FTC cybersecurity resolutions.
- The FTC's FY 2019 cybersecurity consent orders contained two notable new injunctive provisions:
  - –Requirement that a senior officer annually certify to the FTC compliance with the consent order; and
  - –Prohibition on misrepresentations to third parties assessing data security.
- FTC consent orders continued to impose data security and cybersecurity requirements on settling companies for 20 years.

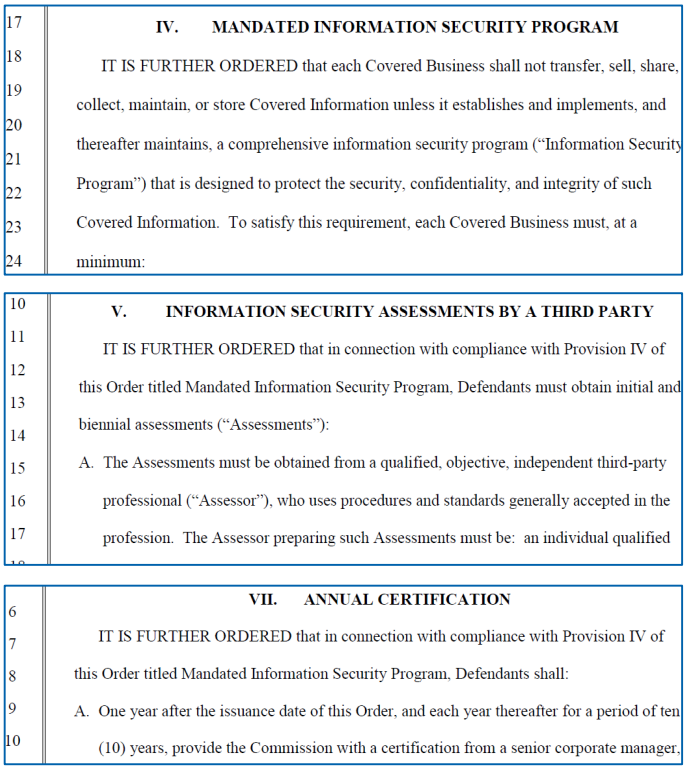
"There is no one-size-fits-all data security program, and the fact of a breach does not necessarily mean that a company's security was unreasonable. . . . The Commission considers whether a company's data security measures are reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its operations, and the cost of tools available to reduce data security risks."

– Andrew Smith, Director of the FTC Bureau of Consumer Protection, Mar. 7, 2019

Cyber Risks, Data Privacy, and Security

Regulatory Developments: FTC

- FTC leadership has emphasized as a key goal strengthening the FTC's orders in data security cases, citing "three major changes" that have achieved the twin objectives of improving data security practices and providing greater deterrence:
  - **More specific orders**. The FTC updated language used in data security orders to now require that companies implement specific measures in response to the issues identified in the complaint.
  - **Increased accountability of third-party assessors**. FTC orders now implement more rigorous requirements for assessor evaluations of order-required comprehensive data security programs, and give the FTC authority to approve and re-approve assessors every two years.
  - **Elevation of data security considerations to the C-Suite and board levels**. In addition to the new annual compliance certifications, companies now are required to present the written information security program to board-level governance.



IV. MANDATED INFORMATION SECURITY PROGRAM

IT IS FURTHER ORDERED that each Covered Business shall not transfer, sell, share, collect, maintain, or store Covered Information unless it establishes and implements, and thereafter maintains, a comprehensive information security program ("Information Security Program") that is designed to protect the security, confidentiality, and integrity of such Covered Information. To satisfy this requirement, each Covered Business must, at a minimum:

V. INFORMATION SECURITY ASSESSMENTS BY A THIRD PARTY

IT IS FURTHER ORDERED that in connection with compliance with Provision IV of this Order titled Mandated Information Security Program, Defendants must obtain initial and biennial assessments ("Assessments"):

A. The Assessments must be obtained from a qualified, objective, independent third-party professional ("Assessor"), who uses procedures and standards generally accepted in the profession. The Assessor preparing such Assessments must be: an individual qualified

VII. ANNUAL CERTIFICATION

IT IS FURTHER ORDERED that in connection with compliance with Provision IV of this Order titled Mandated Information Security Program, Defendants shall:

A. One year after the issuance date of this Order, and each year thereafter for a period of ten (10) years, provide the Commission with a certification from a senior corporate manager,

[i-Dressup Stipulated Order, Apr. 24, 2019]

Cyber Risks, Data Privacy, and Security

Regulatory Developments: California Consumer Privacy Act

- The California Consumer Privacy Act of 2018 ("CCPA") became effective on January 1, 2020.
- Regulations are still being drafted, but the private right of action for certain data breaches began on January 1, 2020.
  - –California residents may sue for statutory damages based on a breach of certain personal information resulting from a business's lack of "reasonable security procedures and practices appropriate to the nature of the information."
- The CCPA requires covered businesses to disclose information to California residents about the categories of personal information they collect, the purposes and uses of that information, whether they share and/or sell that information (and to whom), the rights California residents are granted under the statute, and how residents can exercise those rights.
  - –Whether a business is covered by the CCPA depends on factors including revenue, number of consumers, how personal information is used, and whether the company is operating solely as a service provider.
- Understanding a company's CCPA obligations requires analyzing whether the information falls under exemptions based on sector-specific laws (e.g., GLBA, HIPAA), and whether the personal information falls under temporary and incomplete exemptions added to the CCPA by amendment.

Cyber Risks, Data Privacy, and Security

Criminal Consequences of Cyber Issues

- Through the China Initiative, DOJ continues to focus on countering Chinese and China-related trade secret theft cases, including those based on cyber intrusions.
- DOJ continues to prosecute a range of cyber crime cases, which in 2019 resulted in sentencing of:
  - –Two members of a Romanian cybercrime enterprise to 20 and 18 years' imprisonment, respectively, related to infecting more than 400,000 victim computers with malware;
  - –A businessman at a Chicago manufacturing firm for attempting to download proprietary electronic information from the company where he was employed, and attempting to bring the information to a new company in China; and
  - –A former hedge fund manager to five years' imprisonment for his role in hacking newswire services to steal press releases containing non-public financial information.
- The FBI has begun outreach warning universities of Chinese cybersecurity and espionage threats, and encouraging them to increase oversight of Chinese researchers.

"China wants the fruits of America's brainpower to harvest the seeds of its planned economic dominance. Preventing this from happening will take all of us, here at the Justice Department, across the U.S. government, and within the private sector. With the Attorney General's initiative, we will confront China's malign behaviors and encourage them to conduct themselves as they aspire to be: one of the world's leading nations."

– John Demers, Assistant Attorney General for National Security, July 2, 2019

Cyber Risks, Data Privacy, and Security

UK and European Developments

- The Council of the EU adopted a new EU Cybersecurity Act in March for the regulation of the European Union Agency for Network and Information Security.
- The 2019 Cyber Security Breaches Survey showed that 32% of businesses in the UK identified a cyberattack or a breach in the preceding 12 months—down from 43% the previous year. The survey stated that an attack now costs businesses an average of £4,180 (~$1,300).
- Companies face a tough choice whether or not to pay:
  - A Norway-based aluminium producer, Norsk Hydro, was subject to a ransomware attack in March 2019 that hit 22,000 computers across 170 sites in 40 different countries. The attack led to the company halting production lines. It did not pay the ransom, and the stoppage reportedly cost the company £45 million (~$58 million) in the first quarter of 2019.
  - In December 2019, an FX company, Travelex, identified malware in its systems and took its services offline. News reports suggest the company was asked to pay £4.6 million (~$6 million). The attackers claimed that they downloaded customer data, which they threatened to sell online. Travelex has stated that the breach was unsuccessful.

Cyber Risks, Data Privacy, and Security

UK and European Developments

- Since GDPR entered into force in May 2018, ~160,000 data breaches have been notified.
- In 2019, the UK Information Commissioner's Office issued "Notices of Intention to Fine" ("NOI") for what would be the largest fines imposed under GDPR:
  - British Airways received an NOI to issue a £183 million (~$240 million) fine for security failures (~1.5% of annual turnover).
  - Marriott International received an NOI to issue a £99 million (~$130 million) fine following a data breach (~3% of annual turnover).
- Google was fined €50 million (~$55 million) by the French data regulator after a finding that the company had no sufficient legal basis for processing data for personalized advertisements.
- Authorities will continue to focus on companies' data and records retention practices.
  - The Berlin data protection authority imposed a fine of €14.5 million (~$16 million) on Deutsche Wohnen SE for not having a proper data retention schedule in place. The Danish regulator imposed fines against two companies for similar offenses.
- In December 2019, the Advocate General of the ECJ raised serious doubts over the validity of the "Privacy Shield" (i.e., the mechanism used by thousands of companies to authorize EU/U.S. personal data transfers).

Under the GDPR, European authorities are entitled to impose fines of up to 4% of a company's annual global **revenue (i.e., rather than profits).**

GIBSON DUNN

Foreign Investment in the United States

Foreign Investment in the United States
FIRRMA Update

- The Treasury Department kicked off the new year by issuing new foreign investment regulations, effective February 13, 2020, to implement the 2018 Foreign Investment Risk Review Modernization Act ("FIRRMA").
- FIRRMA expanded the scope of transactions subject to Committee on Foreign Investment in the United States ("CFIUS") review to include:
  - Certain types of non-controlling foreign investments in U.S. businesses that deal with critical infrastructure, critical technology, or the personal data of U.S. citizens ("TID businesses"); and
  - Real estate transactions involving air or maritime ports, or in close proximity to specified U.S. government facilities.
- The new regulations further underscore the growing importance of cross-national cooperation.
  - In designating Australia, Canada, and the UK as the first "excepted foreign states" from which certain investors will receive less scrutiny, the Treasury Department chose countries with "robust intelligence-sharing and defense industrial base integration mechanisms with the United States."
- The new regulations include an interim rule adopting the "nerve center" test for determining a company's principal place of business. The Treasury Department is accepting comments on this interim rule until February 18, 2020.

GIBSON DUNN

Bank Secrecy Act/ Anti-Money Laundering

Bank Secrecy Act/Anti-Money Laundering

Key Enforcement Agencies: FinCEN Update

- The Financial Crimes Enforcement Network ("FinCEN") launched its new Global Investigations Division. The division will focus on investigating and targeting terrorist finance and money laundering threats by utilizing FinCEN's Bank Secrecy Act ("BSA") authorities and Section 311 powers.
- In May 2019, FinCEN issued guidance on how its regulations apply to convertible virtual currencies. The guidance did not create new regulatory obligations, but rather summarized and applied FinCEN's existing regulations and administrative rulings to the cryptocurrency industry. FinCEN also issued an advisory on how virtual currency can be exploited by criminals and used to support illegal activity.
  - More than 11,000 Suspicious Activity Reports ("SAR") have been filed since FinCEN issued this guidance.
- FinCEN maintained its expanded coverage of Geographic Targeting Orders ("GTO") over 12 metropolitan areas, which include the following cities: Boston; Chicago; Dallas-Fort Worth; Honolulu; Las Vegas; Los Angeles; Miami; New York City; San Antonio; San Diego; San Francisco; and Seattle. The purchase amount threshold remains $300,000.
  - The GTOs do not require reporting for purchases made by publicly-traded U.S. companies. Those real estate purchases will be identified through other business filings.
- FinCEN issued its first civil monetary penalty against a peer-to-peer virtual currency exchanger for failure to register as a money service business and conduct diligence on an anonymous client base.

Bank Secrecy Act/Anti-Money Laundering

Key Enforcement Agencies: NYDFS, FINRA, OCC , & FRB Update

- The New York Department of Financial Services ("NYDFS") rejected the application by a cryptocurrency exchange for a virtual currency license in part because it judged the exchange to have an inadequate BSA/AML/OFAC compliance program.
- NYDFS proposed guidance regarding a model framework that an approved BitLicensee could use to create its own system of listing new digital assets, which, if approved by NYDFS, would allow a BitLicensee to list new digital assets without obtaining prior approval from NYDFS.

- The Financial Industry Regulatory Authority ("FINRA") signaled its intention to assess firm compliance with the Customer Due Diligence Rule in its 2019 Priorities Letter.
- FINRA fined BNP Paribas affiliates $15 million for failing to develop and maintain an AML program to detect suspicious transactions in its penny stock deposits and resales program.

The Office of Comptroller of the Currency ("OCC") issued a consent order of prohibition and a $50,000 civil penalty against the former General Counsel of Rabobank, N.A. in connection with the bank's 2018 guilty plea for BSA violations.

In its November Financial Stability Report, the Federal Reserve Board ("FRB") discussed the AML risks of "stablecoin systems," a form of cryptocurrency tied to an underlying asset or assets. The FRB added that it would closely monitor the development of stablecoin systems.

Bank Secrecy Act/Anti-Money Laundering

Key Trends and Developments

- State and federal regulators focused on:
  - –Regulating cryptocurrency and digital assets by issuing guidance and pursuing enforcement actions; and
  - –The strength of corporate BSA/AML compliance programs.
- 2019 saw fewer standalone BSA/AML criminal enforcement actions, with these issues frequently arising in conjunction with sanctions and FCPA cases.
- FINRA remained an active regulator, announcing numerous fines and sanctions for BSA/AML-related violations in 2019, including two fines of $10 million or more for BSA/AML compliance failures.
- FinCEN resolved only one enforcement action in 2019—against an individual.

Key Trends in BSA/AML Enforcement

- Continued focus from regulators on strength of corporate compliance programs
- Modernizing and increasing agencies' enforcement and investigative resources
- Regulating cryptocurrency and digital assets
- Pursuing sanctions- and FCPA-related enforcement actions where money laundering formed part of the underlying conduct

Bank Secrecy Act/Anti-Money Laundering

Key Developments in Criminal Enforcement

- DOJ announced criminal cases against corporate entities and financial institutions involving BSA/AML misconduct:
  - A Miami-based gold refinery, Republic Metals Corporation, entered into an NPA after cooperating in an investigation into money laundering and BSA violations in the gold refining industry.
  - As part of a larger enforcement action involving multiple law enforcement agencies, DOJ fined Standard Chartered Bank $480 million for sanctions-related violations and extended the bank's DPA for two more years. The bank agreed to strengthen and improve its BSA/AML compliance programs as part of the DPA.
  - DOJ settled a civil forfeiture case against assets worth $700 million. The civil forfeiture case stemmed from corruption and money laundering allegations against 1MDB.
    - The FRB leveled a $1.43 million civil penalty against a senior investment banker in the matter.
  - DOJ revealed a 13-count indictment against Huawei, charging it with conspiracy to commit money laundering, along with other financial crimes.
- A former FinCEN staffer pleaded guilty to conspiracy to make unauthorized disclosures of SARs.
- Enforcers in Europe remained active in 2019:
  - Deutsche Bank agreed to pay €15 million (~$16.5 million) in penalties and forfeiture in connection with a Frankfurt Public Prosecutor investigation into shortcomings in the compliance and filing of suspicious activity reports involving German clients connected to offshore accounts.
  - Two Nordic banks, Nordea and Danske, remain under investigation by authorities for their roles in money-laundering issues involving international customers.

Bank Secrecy Act/Anti-Money Laundering

Key Regulatory and Legislative Developments

- The FRB, the Federal Deposit Insurance Corporation ("FDIC"), FinCEN, and the OCC clarified the BSA reporting requirements for hemp-related businesses in light of the 2018 Farm Bill that directed the U.S. Department of Agriculture to regulate hemp production.
- The CFTC, FinCEN, and the SEC issued a joint statement reminding persons engaged in activities concerning digital assets of their BSA/AML obligations.
- Congressional and regulatory interest has continued in creating rules mandating disclosure of Ultimate Beneficial Ownership ("UBO") information of privately held companies and LLCs to a registry that would be maintained by FinCEN.

"[C]riminals thrive when they have somewhere to hide. And the secrecy behind shell companies—businesses that exist only on paper—is a clear and present danger."

- Kenneth Blanco, FinCEN Director,
Dec. 10, 2019

AML
United Kingdom

- The UK government's July 2019 Economic Crime Plan lists seven priority areas to combat economic crime, including money laundering. The Plan anticipates a commitment to launch a flagship economic crime court in London, increase transparency of beneficial ownership including reforms to Companies House, enhanced FCA and HMRC supervision, and engagement with risk industries.
- In July 2019 the FCA announced that it had open more than 60 AML investigations.
- The NCA reported that it had received a record number of SARs (478,437), a 52.72% increase in requests for a Defence Against Money Laundering.
- In April, the FCA fined an international bank £102 million (~$133 million) for AML breaches—the second largest AML fine ever imposed in the UK.
- In September, HMRC issued its largest-ever fine on an FX company, Touma Foreign Exchange.
  - The company was fined £7.8 million (~$10 million), and a director was banned from acting for any business governed by AML rules.

AML
European Union

- Europe continues to pass new legislation: The Fifth Money Laundering Directive became effective on January 10, 2020, and the Sixth Money Laundering Directive will become effective in December 2020.
- In July 2019, the EC published a report assessing recent alleged money laundering cases involving EU credit institutions, finding "significant shortcomings" regarding implementation and enforcement of the Anti-Money Laundering/Counter Terrorist Financing Rules.
- Since 2012, the European Central Bank has been the prudential supervisor of European banks. But AML supervision is excluded as a "business conduct" issue, which remains the sole responsibility of national authorities, leading to a greater number of calls for a European AML regulator.
- In December 2019, Ministers of Finance of France, Germany, Italy, Latvia, the Netherlands, and Spain issued a joint position paper calling for the creation of a new Money Laundering Regulation that would apply directly across Europe, without the need for Member States to transpose it into domestic law.

". . . The steps taken so far might not be enough to effectively prevent money laundering and terrorist financing in the banking sector. Thus, further steps might be considered by the political authorities to make the AML/CFT framework more effective, particularly for cross-border activities."

– Yves Mersch, Member of the Executive Board of the ECB and Vice-Chair of the Supervisory Board of the ECB, Nov. 15, 2019

GIBSON DUNN

Corporate Governance Issues

Corporate Governance Issues

Statement on the Purpose of a Corporation

- In August 2019, Business Roundtable embraced stakeholder governance in a statement signed by 181 high-profile CEOs.
  - The focus on stakeholder value is premised on the theory that part of the purpose of the corporation is to benefit society as an employer and product/service provider—i.e. that while shareholder value creation is important, it is not the only goal.
    - Stakeholders are broadly defined to include communities, as well as employees, customers, suppliers, and shareholders.
  - Proponents, including some institutional investors, advocate stakeholder governance from the belief that the fiduciary duty of management and the board is to promote the long-term value of the corporation.
  - But detractors have expressed concerns that this approach "undercuts notions of managerial accountability to shareholders."

CORPORATE GOVERNANCE

Business Roundtable Redefines the Purpose of a Corporation to Promote 'An Economy That Serves All Americans'

AUG 19, 2019

Updated Statement Moves Away from Shareholder Primacy, Includes Commitment to All Stakeholders

WASHINGTON – Business Roundtable today announced the release of a new Statement on the Purpose of a Corporation signed by 181 CEOs who commit to lead their companies for the benefit of all stakeholders – customers, employees, suppliers, communities and shareholders.

Corporate Governance Issues

Ascendancy of ESG Considerations: Environmental

- The focus on companies' impact on the communities in which they operate has led to a significant shift in many companies' approach to doing business—and suggests a coming sea change.
- BlackRock CEO Larry Fink recently wrote in his 2020 annual letter to CEOs of a "fundamental reshaping of finance" and a "profound reassessment of risk and asset values" brought about by the need to consider climate change factors that can no longer be ignored.
- Other companies—and regulators—have reached similar conclusions. For example:
  - –Sustainable investment assets are rising, with assets at $30.7 trillion in early 2018 across the major markets of the United States, Europe, Australia, Canada, Japan, and New Zealand—a 34% increase over two years.
  - –In November 2019, the U.S. Chamber of Commerce issued ESG reporting best practices.
  - –In December 2019, the European Parliament finalized a first-of-its-kind agreement to become the first supranational regulator to set standards for whether an economic activity can be considered environmentally sustainable—the "Taxonomy Regulation."

"Climate change is different. Even if only a fraction of the projected impacts is realized, this is a much more structural, long-term crisis. Companies, investors, and governments must prepare for a significant reallocation of capital.."

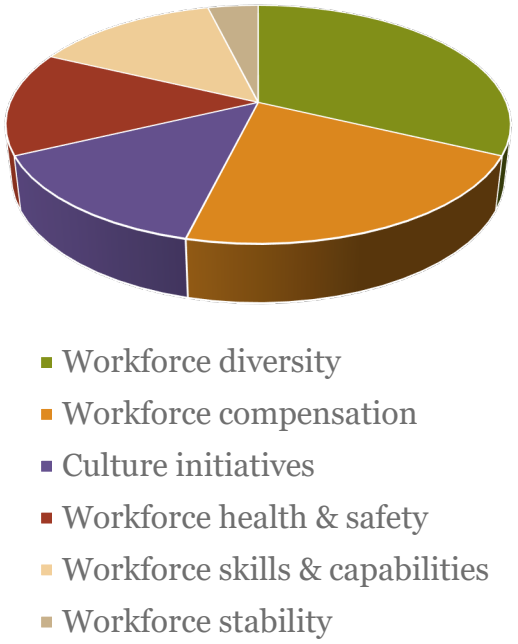
– Larry Fink, BlackRock Chairman and CEO, Jan. 14, 2020

Corporate Governance Issues

Ascendancy of ESG Considerations: Social

- Human capital management has been rapidly emerging as a critical focus area for stakeholders.
- Many Fortune 100 companies are disclosing their governance and management of human capital in corporate responsibility or sustainability reports and in proxy statements. Examples of corporate disclosures include:
  - ~ 30% of companies discussing workforce diversity provided some measure of workforce diversity data.
  - ~40% of companies discussing compensation provided specific performance data around pay equity beyond the required CEO pay ratio disclosure.
  - Just over 40% of the Fortune 100 broadly stated that the board oversees human capital management or culture.
  - Nearly 30% of Fortune 100 companies included human capital-related experience among skills and areas of expertise sought at the board level.
- The SEC has proposed amendments to Item 101 of Regulation S-K to include human capital resources as a disclosure topic for the Business section, to the extent material.

Human Capital Management Topics Most Often Addressed by Fortune 100 companies in 2019 Proxy Statements*

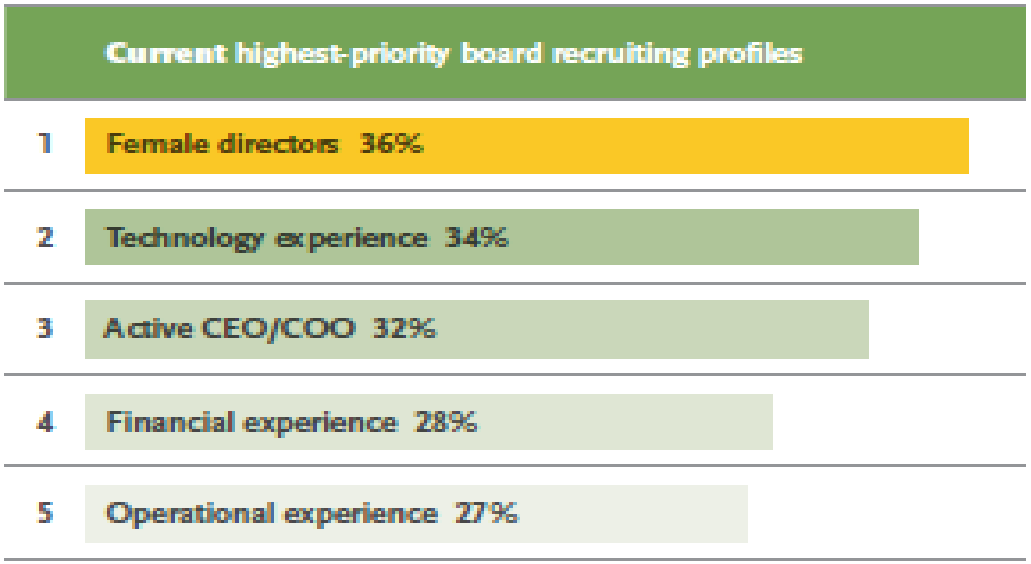


*Information relating to human capital disclosure practices based on Nov. 2019 study by the EY Center for Board Matters.

Corporate Governance Issues

Ascendancy of ESG Considerations: Governance

- **Board Refreshment**
  - –According to a recent survey,* boards are responding to increasing demands from shareholders and other stakeholders to increase boardroom diversity in terms of gender, age, race/ethnicity, and professional backgrounds.
  - –The survey finds that the biggest drivers of board refreshment will be (1) replacing retiring directors (41%) and (2) adding new skills to the board (41%).
  - –Current highest-priority board recruiting profiles are as follows:



"What if we don't change at all ... and something magical just happens?"

*Spencer Stuart Board Index (2019).

Corporate Governance Issues

Focus on ESG Issues and Ratings

- Institutional investors are focused on sustainability. ISS and Glass Lewis voting reports include sustainability ratings/data. This demonstrates keen interest in companies' ESG performance and disclosure. Key topics include human capital management; board evaluations and composition (matrices, tenure, refreshment, and diversity); and sustainability/climate change.
  - –A recent G&A Institute Survey indicates that 86% of S&P 500 companies published sustainability or corporate responsibility reports in 2018, compared to 20% in 2011.
- Following European trends, U.S. investors may be moving towards standardized sustainability disclosures.
  - –A 2019 survey highlighted investor complaints that companies' sustainability disclosures cannot readily be used to inform accurate investment decisions because disclosures vary from company to company and there are no standardized disclosure requirements.
  - –This move has faced pushback from the SEC. Other frameworks, such as the Sustainability Accounting Standards Board, are gaining influence.

"Environmental, particularly climate change, and social factors, in addition to governance, have become material issues for investors to consider when making investment decisions and undertaking stewardship."

– Financial Reporting Council, introduction to the UK Stewardship Code 2020

Corporate Governance Issues

2019 Proxy Season Update and 2020 Expectations

- **Trends among shareholder proposal categories**:

Category	% of total	YoY trend	Largest sub-category
Social	28%	↑9% to 220	Anti-discrimination & diversity (29%)
Environmental	14%	↓22% to 109	Climate change (44%)
Governance	36%	↑3% to 289	Independent chair (22%)
Civic engagement	12%	↑7% to 98	Political contributions (62%)
Executive compensation	7%	Flat at 54	Add ESG metrics to comp (35%)

Shareholder Proposals to Expect in 2020:

- Board diversity (e.g., NYC Comptroller campaign)
- Climate change and other environmental proposals
- Senior executive compensation (including clawbacks and non-GAAP performance metrics)
- Other governance matters, including written consent, independent chair, simple majority voting, purpose of corporation, and shareholder approval of bylaw amendments approved by board

Corporate Governance Issues

Delaware Caremark-Related Cases

Case	Details
In re Caremark International, Inc. Derivative Litigation (Sept. 25, 1996)	The Delaware Court of Chancery concluded that directors can be liable for failures in their oversight duties when there is "a sustained or systematic failure of the board to exercise oversight" or "utter failure to attempt to assure a reasonable information and reporting system exists."
Stone v. Ritter (Nov. 6, 2006)	The Delaware Supreme Court clarified the standard for pleading a *Caremark* claim for oversight failure with two prongs: (1) directors "utterly failed to implement any reporting or information system or controls; *or* (2) having implemented such a system or controls, consciously fail to monitor or oversee its operations thus disabling themselves from being informed of risks or problems requiring their attention."
Reiter v. Fairbank (Oct. 18, 2016)	The Delaware Court of Chancery rejected a shareholder derivative lawsuit by clarifying that good faith, not a good result, is required for directors to fulfill their oversight duties.
Marchand v. Barnhill (June 18, 2019)	The Delaware Supreme Court held that plaintiff had alleged facts supporting a reasonable inference that the company's board "made no effort" to implement a board-level system to monitor the safety of ice cream that led to the death of three people as a result of a listeria outbreak.
In re Clovis Oncology, Inc. (Oct. 1, 2019)	The Delaware Court of Chancery held that, although a company compliance system was in place, the board ignored multiple warning signs that management was inaccurately reporting the drug's efficacy and that the "Board consciously ignored red flags that revealed a mission critical failure."

Corporate Governance Issues

Evolution of Risk Oversight Director Liability (Delaware)

1996
(*Caremark*)

"Sustained or systemic failure of the board to exercise oversight" or "utter failure to attempt to assure a reasonable information and reporting system exists"

1998-2018
(*Stone; Reiter*)

- *Caremark* hurdle rarely satisfied

-Shareholder suits alleging director liability due to oversight failure generally dismissed

2019
(*Marchand; Clovis*)

Potential director liability due to lack of board-level effort in monitoring risk

Corporate Governance Issues

Recent Delaware Caremark-Related Cases

- Board takeaways from *Marchand* and *Clovis*:
  - –Identify critical risks to the company's business and operations, ensure that appropriate board-level reporting systems are in place for each critical risk, and rigorously exercise oversight when a company operates in an environment where externally imposed regulations govern its "mission critical" operations;
  - –Carefully and thoroughly document those risks (and any yellow or red flags raised in relation to them);
  - –Assess whether directors have sufficient expertise to engage with management on critical risks; and
  - –Determine whether each critical risk can be managed by the board or an existing board committee, or if a new standing committee would aid the board in performing its oversight function.
    - Companies should be vigilant in tracking evolving legislation that can affect their business litigation risks, and must evolve their compliance systems accordingly.

Corporate Governance Issues

Update on Section 220 Demand Litigation

Section 220 of the Delaware General Corporation Law gives stockholders of Delaware corporations the ability to inspect certain corporate books and records where they have a "proper purpose" to seek these materials.

- Several 2019 Delaware opinions likely will amplify the recent increase in 220 demands:
  - In *KT4 Partners LLC v. Palantir Technologies Inc.*, the Supreme Court held that the Court of Chancery abused its discretion in refusing to allow the plaintiff to inspect emails in response to a books and records inspection demand.
  - The Court of Chancery held in *In re Oracle Corporation Derivative Litigation* that the lead plaintiff in a shareholder derivative suit could subpoena documents (including certain privileged documents) produced by Oracle and relied upon by the company's special litigation committee.
  - The Court of Chancery allowed stockholders access to AmerisourceBergen Corp. formal board materials regarding corporate compliance with opioid drug controls, observing that the "flood of government investigations and lawsuits" into the company provided a credible basis to suspect corporate wrongdoing warranting further investigation.
- Earlier in 2019, however, in *High River LP et al. v. Occidental Petroleum Corp.*, the Court of Chancery rejected an interpretation of Section 220 that would expand the "proper purpose" test to include communication with other stockholders in connection with a potential proxy contest, noting that it would "invite mischief to open corporate management to indiscriminate fishing expeditions."

Corporate Governance Issues
Board Diversity

- **Congressional Hearing on Board Diversity**: The June 2019 hearing examined options for diversifying gender, racial, and ethnic composition of corporate boards, including adoption of a "Rooney Rule" approach to expand the director candidate pool beyond CEOs and corporate America and include candidates from other backgrounds, as well as regularly analyze diversity data to identify diversity deficiencies and best practices.
- **State Legislation**
  - *California*: Conservative nonprofit Judicial Watch filed a lawsuit challenging California's board diversity law (SB 826)—which requires a minimum number of female directors on the boards of public companies with principal executive offices in California—on the grounds that it violates the equal protection provisions of the California Constitution by employing a gender-based quota.
  - *Illinois*: The Governor of Illinois signed legislation requiring publicly-traded companies with their principal offices in Illinois to include information about board and executive officer diversity in their annual reports filed with the Secretary of State, beginning in 2020.
- **Call for Companies to Implement the Rooney Rule**: The NYC Comptroller launched the Boardroom Accountability Project 3.0 in October 2019, calling on companies to adopt a policy requiring the consideration of women and people of color for not only every open board seat, but also for the CEO position.

Corporate Governance Issues

New SEC Guidance Regarding Shareholder Proposals

- **Significant Changes to the No-Action Letter Process**
  - SEC Staff now may respond orally or in writing to shareholder proposal no-action requests.
    - The Staff have indicated that they intend to issue a written response letter where they "believe[] doing so would provide value, such as more broadly applicable guidance about complying with Rule 14a-8."
    - The Staff have created a chart on the Division of Corporate Finance's website reporting on the disposition of their responses to no-action requests.
  - In some cases, no definitive response will be provided by the Staff.
    - The Staff have stated that parties should not interpret this as indicating that the proposal must be included.
    - These situations may be limited to those where the Staff are not in the best position to make a decision about excludability of the proposal.
  - If the Staff decline to state their views on a proposal, companies will need to decide whether or not to exclude the proposal from their proxy statements. Exclusion of a proposal without a decision by the Staff could lead to proponents suing the company in federal court.

Corporate Governance Issues

New SEC Guidance to Audit Committees

- In a rare move, the SEC published in December 2019 a "Statement on Role of Audit Committees in Financial Reporting and Key Reminders Regarding Oversight Responsibilities."
- The Statement discusses best practices for audit committees and is presented as "observations and reminders [to] assist audit committees carrying out their year-end work":
  - –Tone at the Top;
  - –Auditor Independence;
  - –Generally Accepted Accounting Principles ("GAAP") Measures;
  - –Non-GAAP Measures;
  - –ICFR;
  - –Communications to the Independent Auditor;
  - –Reference Rate Reform (LIBOR); and
  - –CAMs.

> *"The strength of our capital markets, and the confidence of investors in our markets, is driven by the continued quality and reliability of financial reporting. Independent audit committees perform a vital role . . . ."*
>
> – SEC Statement, Dec. 30, 2019

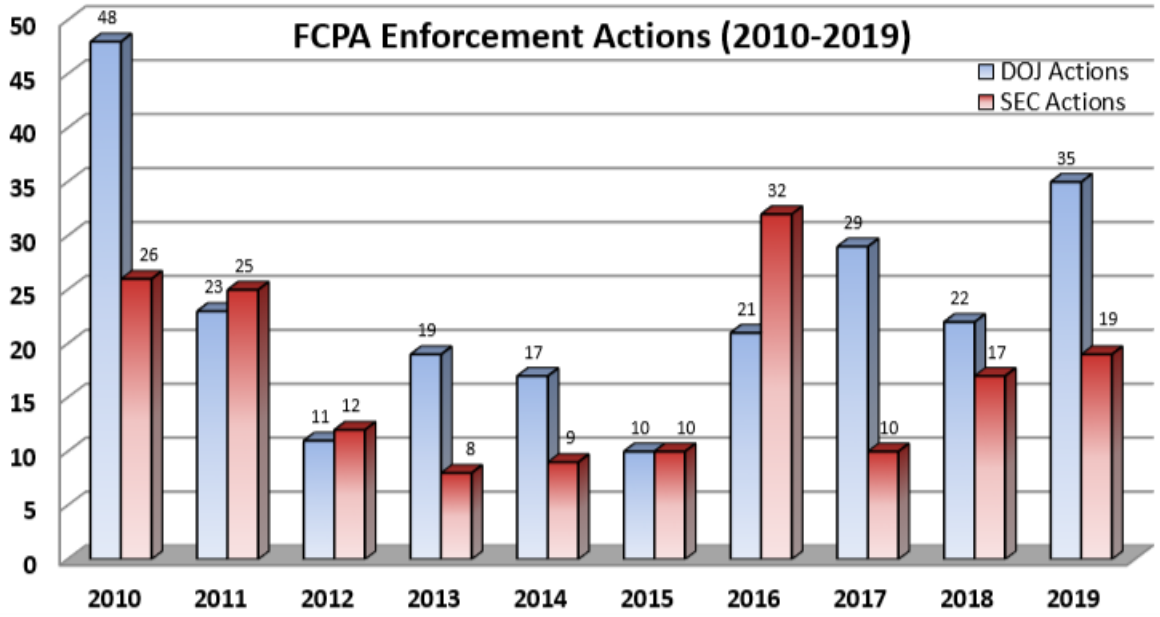
GIBSON DUNN

White Collar and Securities Fraud

White Collar and Securities Fraud

FCPA Enforcement by the Numbers

- 2019 marked a significant year in FCPA enforcement, with 54 combined FCPA enforcement actions and more than $2.6 billion in corporate fines—a new record driven by the two largest corporate FCPA monetary resolutions to date.
- DOJ FCPA enforcement, in particular, focused on individual rather than corporate actors.
  - –The SEC and DOJ announced FCPA charges against 30 individuals in 2019, and DOJ initiated an additional 19 individual prosecutions in non-FCPA actions arising out of FCPA investigations.

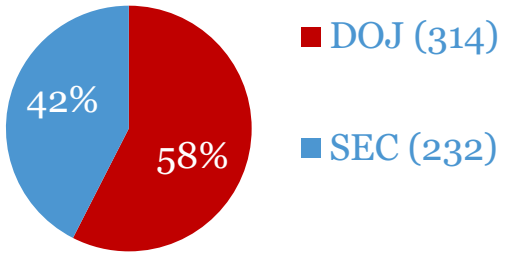


White Collar and Securities Fraud

DOJ and SEC FCPA Enforcement

- The SEC settled 13 enforcement actions against companies this year, including two blockbuster settlements with parallel DOJ actions resulting in DOJ/SEC combined monetary resolutions of $850 million and more than $1 billion, respectively.
- DOJ secured four guilty pleas from corporate defendants in FCPA actions and reached three NPAs and four DPAs with corporations.
- DOJ revised its FCPA Corporate Enforcement Policy twice this year:
  - –In March, DOJ reversed course on requiring companies to ban the use of disappearing messaging services to receive full credit for remediation.
    - The policy now requires companies to implement internal guidance and controls on the use of such services.
  - –In November, DOJ clarified what information companies seeking a declination must disclose and when.
- DOJ issued two declinations under the FCPA Corporate Enforcement Policy—since the policy went into effect in 2016, there have been 13 total declinations.

Total FCPA Enforcement Actions: 2005 - 2019



White Collar and Securities Fraud

United Kingdom Update

- 2019 saw three convictions (all guilty pleas) in separate Serious Fraud Office ("SFO") bribery and corruption cases, and six acquittals. There were two SFO convictions for fraud-related offenses, and two acquittals.
- In 2018/2019, the SFO secured over £10 million (~$13 million) in new financial orders, with payments received against orders of more than £8 million (~$10.5 million).
- The SFO now has finalized a total of six DPAs, with a seventh reportedly on the way:

2015	2016	2017	2018	2019
1	1	2	0	2

- The SFO closed a number of long-running investigations.

"Prosecutors all around the world are realising how much we need each other if we are truly to do justice. So we are increasingly linking arms in the march against transnational fraud and corruption."

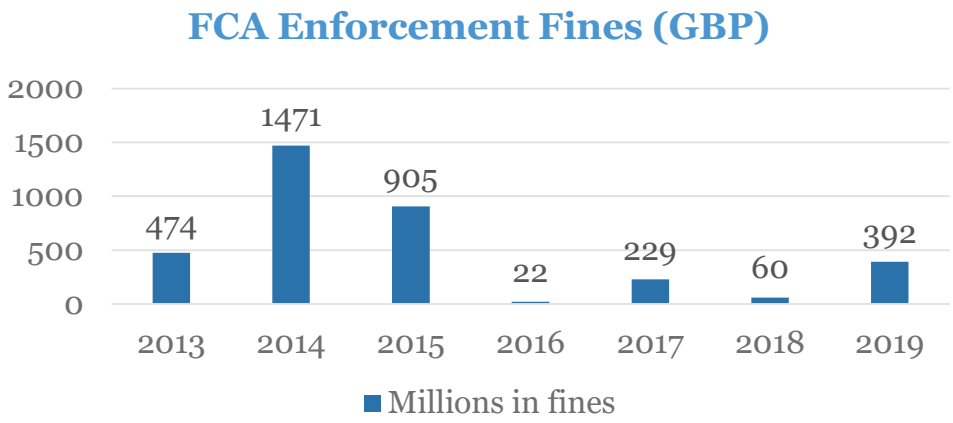
– Lisa Osofsky,
SFO Director,
Sept. 2, 2019

- The SFO released its "Corporate Co-Operation Guidance," which sets out its expectations for companies hoping to enter into a DPA.
- The SFO also released additional guidance for prosecutors on "Evaluating a Compliance Programme." The Guidance illustrates that the SFO will, early in any investigation, actively investigate the state of a company's systems and controls.

White Collar and Securities Fraud

United Kingdom Update – Financial Services

- The Financial Conduct Authority ("FCA") opened more enforcement cases during 2018/2019 than the previous period.
- The average length and cost of all regulatory and civil cases (including those closed with no further action) has fallen from the preceding period. The average length and cost of criminal cases has increased.



- In 2019, the FCA issued fines to 15 companies and six individuals.
  - –The largest fine issued to a company: £102 million (~$133 million).
  - –The largest fine issued to an individual: £76 million (~$100 million).
- In July 2019, a jury found two individuals guilty of insider dealing offenses, following an FCA investigation and prosecution. Both were sentenced to three years' imprisonment. The FCA likely will take confiscation proceedings against both individuals.
- The Senior Managers' Certification Regime will focus the FCA on management accountability.

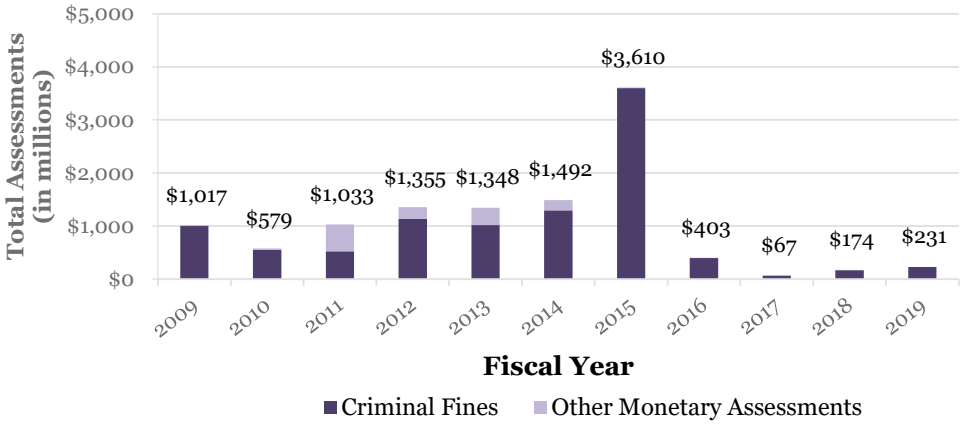
GIBSON DUNN

Antitrust

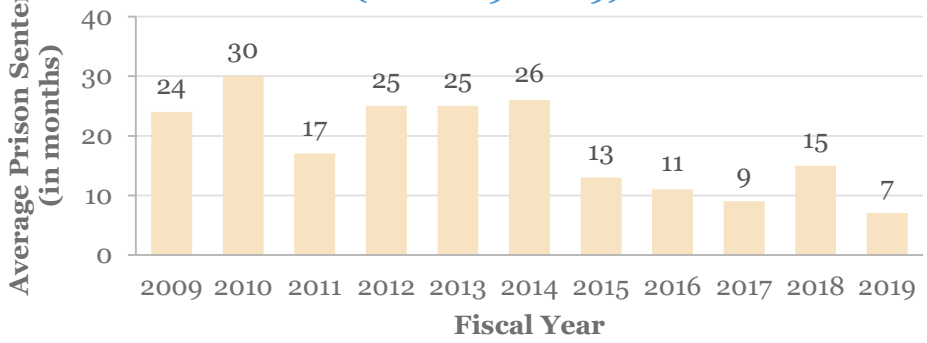
Antitrust
U.S. Update

- In July 2019, DOJ began to take corporate compliance programs into account at the charging phase of criminal antitrust investigations, rather than only at sentencing.
- DOJ's largest FY 2019 criminal antitrust initiative focused on alleged bid-rigging in fuel contracts for U.S. military bases in South Korea.
  - Two coordinated criminal and civil resolutions in November 2018 and March 2019 resulted in five companies paying more than $350 million in fines and damages.
  - Departing from the usual strategy in recent years, DOJ used Section 4 of the Clayton Act to obtain antitrust damages in these cases.
- DOJ also continued antitrust enforcement related to packaged seafood in FY 2019, obtaining a statutory maximum $100 million fine against StarKist and a trial conviction of another company's former executive for conspiracy.

Total Criminal Fines & Other Monetary Assessments from Antitrust Division Corporate Resolutions (FY 2009–2019)



Average Length of Prison Sentence (FY 2009–2019)

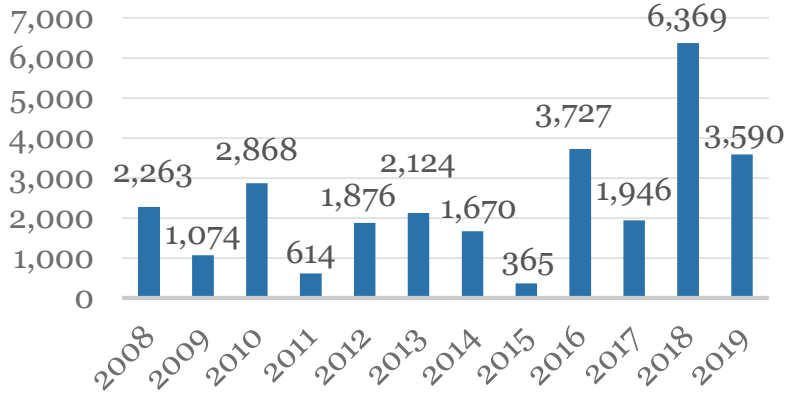


Antitrust

European Union and UK Update

- 2019 saw significant antitrust fines in the EU:
  - In March, the European Commission fined Google ~€1.5 billion (~$1.6 billion) for abusing its market dominance by imposing restrictive clauses in third-party contracts.
  - In May, the European Commission fined a number of banks a combined €1.2 billion (~$1.3 billion) for taking part in a cartel in the foreign exchange market.
- The UK government has published guidance on the CMA's role after the UK leaves Europe.

Fines Levied by the EC (€ in millions) 2008 – 2019



- In April, the UK Court of Appeal ruled that the Competition Appeal Tribunal (the "CAT") had erred in refusing to grant a collective proceedings order ("CPO") to bring a collective action against Mastercard in relation to interchange fees, a case worth an estimated £14 billion (~$18 billion). The Supreme Court is due to hear an appeal from Mastercard in May 2020.
- An application for a CPO was launched in the CAT against five banks in July, following two European Commission settlements concerning the spot FX market. A second overlapping application for a CPO was launched in the CAT against six banks in December.
- In October, the CAT held that the funding arrangements of the proposed class representatives in the collective actions relating to the "trucks" cartel were adequate for the purpose of determining the suitability of the proposed class representatives.

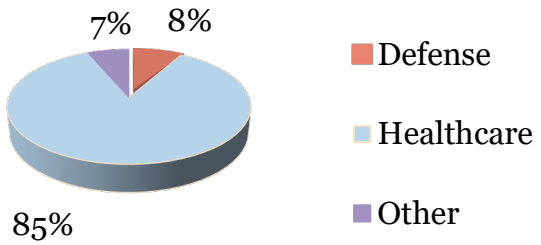
GIBSON DUNN

False Claims Act

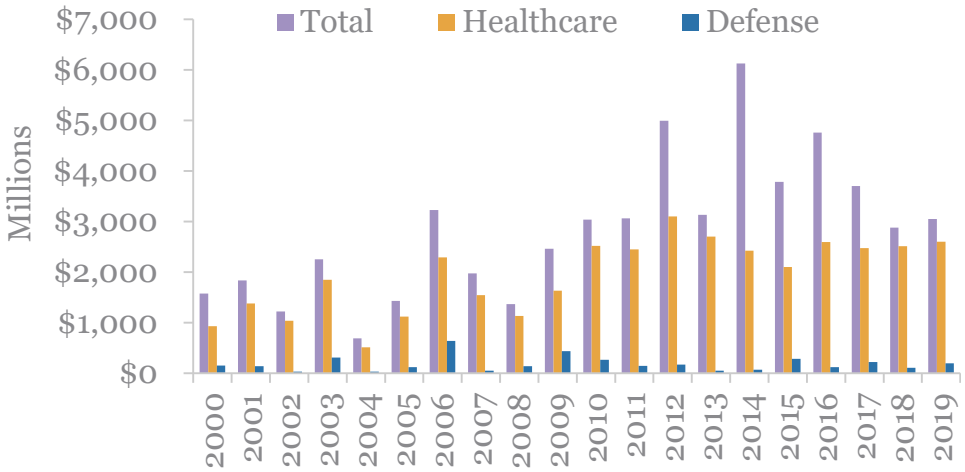
False Claims Act

- False Claims Act ("FCA") recoveries exceeded $3 billion in 2019, a slight uptick from the $2.8 billion recovered in 2018.
- Federal legislative and regulatory activity remained quiet; the future of the Affordable Care Act ("ACA"), and the ACA's amendments to the FCA, are uncertain due to the Fifth Circuit holding the individual mandate unconstitutional but remanding for further proceedings on severability.
- The U.S. Department of Health and Human Services approved six states' false claims statutes, which permit the states to receive a 10% increase in the share of recoveries.

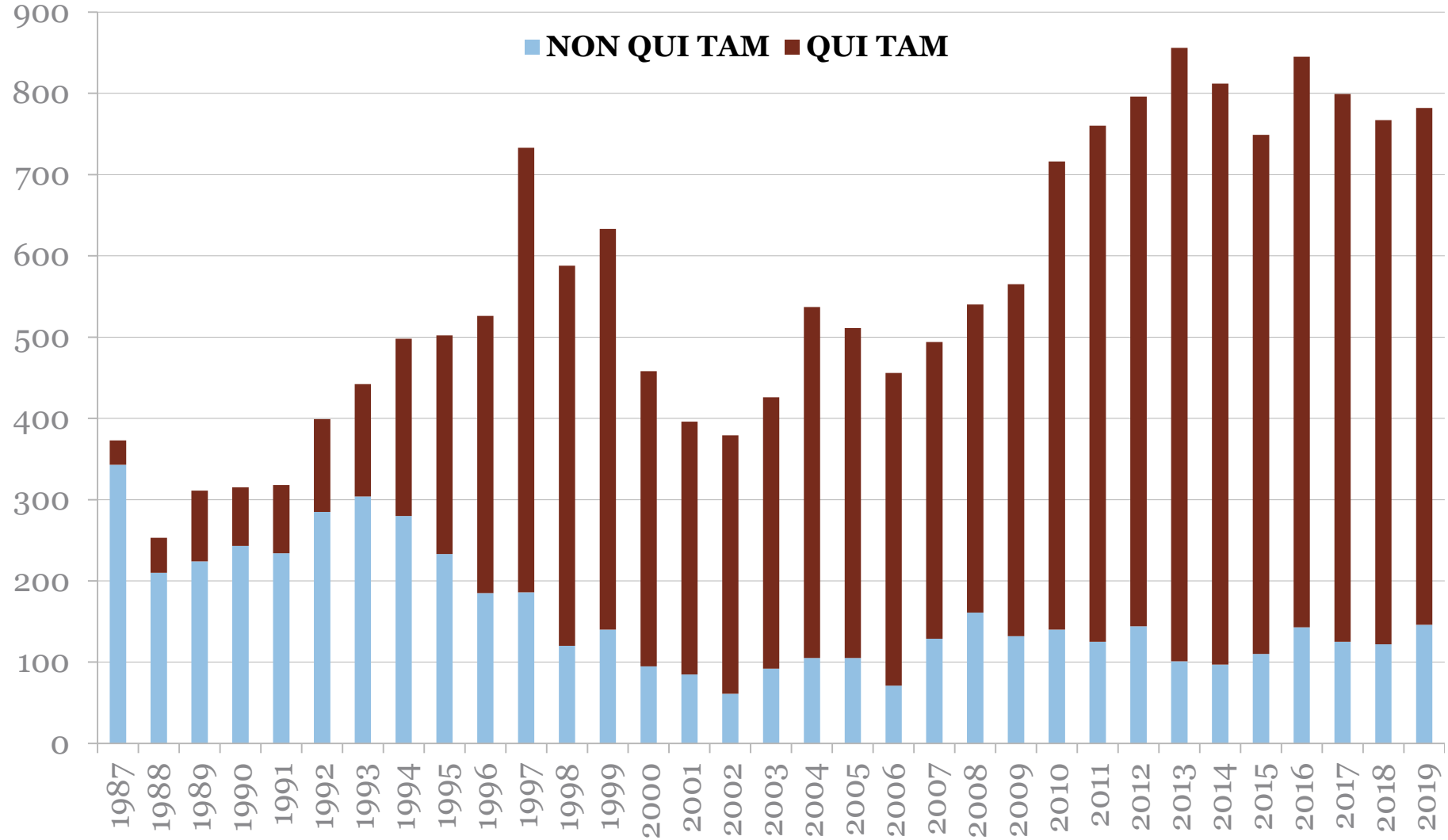
FCA Recoveries from the Defense and Healthcare Industries



Annual FCA Recoveries by Industry



False Claims Act Annual New Matters (1987 – 2019)



False Claims Act Policy Developments

- **Cooperation Guidance**: In May, DOJ issued guidance on cooperation credit to targets of FCA enforcement.
  - Voluntary self-disclosure yields maximum benefit and cooperation credit capped at no less than single damages. The guidance gives DOJ significant discretion; it is not yet certain which way that discretion cuts.
- **Granston Memo** (now codified in Justice Manual): DOJ filed more motions to dismiss in 2019, including on the basis that relators' allegations were weak. But DOJ signaled that seeking dismissal will remain the exception, not the rule, and will be based on a cost-benefit analysis centered on the likely success of relator's claim.
  - In September, Senator Grassley raised concerns that the Granston memo undercuts the FCA by permitting dismissal based on "vague" guidance and "questionable concerns over" "limited government resources."

"Just because a case may impose substantial discovery obligations on the government does not necessarily mean it is a candidate for dismissal."

– Michael Granston,
then-Director, Civil Fraud Section,
Civil Division Department of Justice
Feb. 28, 2019

"Seemingly in response to the Granston memo, DOJ has moved to dismiss or threaten to dismiss several cases at least in part because of litigation costs, even though its arguments were vague, pretextual and could not demonstrate cost was prohibitive."

– Senator Chuck Grassley,
Sept. 4, 2019

False Claims Act Policy Developments

- In October, the Federal Housing Administration ("FHA") and DOJ signed a Memorandum of Understanding ("MOU") that provides guidance on using the FCA to enforce FHA regulatory requirements.
    - The MOU follows at least 14 settlements between 2015 and 2019 related to FHA mortgage insurance programs, totaling more than $1 billion.
- The MOU seeks to encourage greater bank and lending institution participation in FHA programs by enforcing violations of FHA program requirements "primarily through [the U.S. Department of Housing and Urban Development ("HUD")]'s administrative proceedings," rather than the FCA.
- Under the MOU, HUD may refer a matter to DOJ to pursue FCA claims when two conditions are met:

> *"[T]he False Claims Act became a monster that started chasing everybody around the room, making their lives miserable and causing them an inordinate amount of pain [with this MOU the FCA] monster has been slayed."*
>
> – Ben Carson, Secretary of Housing and Urban Development, Oct. 28, 2019

1. The most serious violations ("Tier 1" violations under HUD regulations) exist either: (a) in at least 15 loans or (b) in loans with an unpaid principal balance of at least $2 million; and
2. There are aggravating factors, such as evidence that the violations are systemic or widespread.

False Claims Act Notable Decisions

- In *Cochise Consultancy, Inc. v. United States ex rel. Hunt*, the Supreme Court resolved a circuit split and held that relators pursing cases in which the government declined to intervene can take advantage of the FCA's longer statute of limitations, which extends up to 10 years after the relevant U.S. official knew or should have known the relevant facts.
- Circuits continue to interpret the FCA's materiality requirement post-*Escobar*, and are beginning to converge on a number of non-dispositive factors, including:
  - Whether the government expressly conditioned payment on meeting relevant requirements;
  - Whether the government would have denied payment had it known relevant information; and
    - To determine this, courts have looked to the government's past enforcement actions regarding the relevant provision and whether the government intervened in the case.
  - Whether non-compliance was insubstantial or minor or, in contrast, goes to the very essence of the bargain.
- The Supreme Court again declined a petition for *certiorari* requesting to clarify *Escobar*'s materiality standard.

False Claims Act Notable Cases

- Combating the opioid epidemic remains an enforcement priority. Jody Hunt, Assistant Attorney General, Civil Division, recently reaffirmed that DOJ "is committed to using the legal tools at [its] disposal to combat the illegal marketing and distribution of opioids, including fentanyl."
- To this end, two of the largest 2019 FCA settlements related to opioids:
  - As part of a $1.4 billion global resolution, Reckitt Benckiser paid $700 million to resolve claims that a formerly held subsidiary marketed an opioid treatment and caused false claims to be submitted to government health care programs.
  - Insys, an opioid manufacturing company, paid $225 million to resolve criminal and civil investigations, $195 million of which resolved five FCA cases.
- The government intervened in an FCA case against a large pharmaceutical company, Mallinckrodt, alleging that the company used a foundation as a conduit to pay illegal kickbacks in the form of co-pay subsidies so it could market the drug as "free" to doctors and, at the same time, increase its price.
  - The same drug manufacturer paid $15 million to the government to resolve claims it paid illegal kickbacks to doctors via dinners and entertainment to induce prescriptions.

GIBSON DUNN

Criminal Tax and Cross-Border Concerns

Criminal Tax and Cross-Border Concerns
U.S. Update

- HSBC Private Bank was scrutinized by investigators regarding tax avoidance advice.
  - –As part of a DPA, the bank agreed to pay $192.35 million, including $60.6 million in restitution to the Internal Revenue Service ("IRS"); $71.85 million in fees the bank earned on undeclared U.S. bank accounts; and a $59.9 million penalty.
  - –DOJ took into account that the bank self-reported these violations, conducted an internal investigation, provided extensive cooperation, and took remedial action.
- DOJ obtained a $195 million payment from an Israeli bank as part of a DPA to settle charges of tax evasion by certain former, low-level employees enabling violations of U.S. law by American customers.
- DOJ entered into an NPA with a Swiss-based private bank stemming from the bank's efforts to conceal the assets and income of U.S. clients from the IRS. The bank agreed to pay a $10.6 million penalty as part of the resolution.
- Pursuant to a treaty with Finland, a federal court authorized the IRS to serve John Doe summonses on three banks. The summonses sought information from those banks about persons in Finland with payment cards are linked to bank accounts outside of Finland.
- DOJ signed addendums to two NPAs that originally were entered into as part of the Swiss Bank Program in 2015.

GIBSON DUNN

Building and Overseeing Effective Compliance

Top Compliance Concerns

- As a recent survey indicates, compliance professionals' compliance concerns moving into a new decade remain similar to previous years:
  - –Top anticipated risks for 2020 include the impact of regulatory change, succession challenges, cyber threats, and privacy and information security.
  - –Of the top ten concerns, six related to operational risk areas—cyber threats, succession challenges, ability to compete with new competitors, encouraging timely identification and escalation of risk issues, and the like.

TOP RISKS FOR 2020
1. Impact of regulatory change and scrutiny on operational resilience, products and services
2. Economic conditions impacting growth
3. Succession challenges; ability to attract and retain top talent
4. Ability to compete with "born digital" and other competitors
5. Resistance to change operations
6. Cyber threats
7. Privacy/identity management and information security
8. Organization's culture may not sufficiently encourage timely identification and escalation of risk issues
9. Sustaining customer loyalty and retention
10. Adoption of digital technologies may require new skills or significant efforts to upskill/reskill existing employees *(new in 2020)*

*Protiviti, Illuminating the Top Global Risks in 2020

Gatekeeper Liability Continues

- Regulators continue to penalize gatekeepers for both actively facilitating and passively allowing compliance failures at their organizations.
  - DOJ investigates and prosecutes compliance professionals for allegedly inappropriate facilitation of, or participation in, misconduct, and for failing to satisfy professional standards.
  - Companies should ensure that gatekeepers receive appropriate guidance and training to be effective.

- In February 2019, DOJ announced the indictment of the former president and chief legal officer of an IT services company for facilitating bribes paid to a government official. DOJ alleged that:
  - The company's then-president and chief legal officer, who also oversaw and managed the company's compliance functions, authorized the bribes.
  - After authorizing the bribes, they directed company personnel to conceal the bribes by falsifying documents.
- DOJ declined to prosecute the company under its FCPA Corporate Enforcement Policy.

- The updated DOJ Evaluation of Corporate Compliance Programs specifically notes that prosecutors should consider the role of gatekeepers.

"Gatekeepers play a critical role in our markets, and policing their misconduct is a critical part of our mission."

– SEC Division of Enforcement
2019 Annual Report

Designing the Compliance Program

Core Elements of an Effective Program

Per DOJ's updated guidance, prosecutors (and companies) should consider whether the program:

1. Is a well-designed program
   - *Risk-based, with clearly defined policies and procedures, effective training and communication, reporting channels and investigations capabilities, third-party diligence process, M&A pre-acquisition due diligence and post-acquisition integration processes.*

2. Is being applied earnestly and in good faith—i.e., implemented effectively
   - *Commitment by senior and middle management to a culture of compliance, appropriately appointed compliance function, with clear and consistent disciplinary procedures and incentives for ethical behavior.*

3. Works in practice
   - *Continuous assessment and improvement of the program, including via review and investigation of root causes, with appropriate remedial action and discipline for supervisory failures.*

Risk Assessment

- Effective risk assessment can both prevent misconduct, by identifying and addressing areas of greater exposure for the company, and demonstrate to regulators that the company is committed to addressing potential compliance risks.

Spotlight on Cyber

- Companies should assess meaningful changes to board-level governance of technology-related risks, including data-related risks such as:
  - Adequacy and performance of corporate technologies, including sufficient resources to support them;
  - Emerging technologies that could enhance the corporate mission—or, conversely, render it obsolete; and
  - Ethical considerations associated with technology.
- Companies should also consider technology experience and expertise as important director qualifications.

Hallmarks of Effective Risk Assessment

- Tailored to particular risk areas
- Focused, but not myopic, taking into account different stakeholder perspectives
- Incorporates ongoing monitoring and analysis of results
- Ensures organizational resources sufficient to identify and address potential exposure
- Monitors key regulatory developments and rapidly changing compliance expectations

* Deloitte Boardroom Agenda (2020).

Risk Oversight

- Board oversight of material risks should be addressed through ongoing, documented evaluation by the board and its committees.
- Risk should be a significant part of a board's:
  - Evaluation of strategy;
  - Consideration of significant transactions;
  - Evaluation of management effectiveness; and
  - Oversight of crisis preparedness.

"[A] board [must] make a good faith effort to put in place a reasonable system of monitoring and reporting about the corporation's central compliance risks."

- *Marchand v. Barnhill* (June 18, 2019)

- ✓ *Review material risks with management on a regular basis*
- ✓ *Evaluate current structures and resource allotments with respect to risk assessment and mitigation processes*
- ✓ *Document compliance efforts and risk monitoring mechanisms in board minutes and meeting materials*
- ✓ *Consider public disclosures of material risks overseen by the board*

Communicating (is Creating) the Culture of Compliance

- The compliance dialogue drives and supports a compliance culture. Instilling a corporate dialogue that values and emphasizes the value of compliance is particularly difficult—and important—for companies whose operations and offices span different countries and languages. Companies have addressed this challenge in a number of different ways:

  - Including a compliance-related message in annual communications from the board level/C-Suite, and more frequent compliance messaging from senior and middle management.
  - Establishing a "compliance month" with programming around the value of compliance and compliance examples (and emphasizing the importance of compliance during every month of the year with a compliance message every week).
  - Making mandatory trainings engaging and interactive—for example, hypothetical scenarios that ask employees how they would react when exposed to a situation that presents compliance risk.
  - Providing public recognition to employees who have met compliance challenges appropriately (and circulation of public examples where they have not, such as messaging regarding recent relevant enforcement actions).
  - Emphasizing compliance as a centerpiece of regular all-hands or town hall meetings.

Focus on Internal Audit – a Sword and Shield

- A number of recent enforcement actions increasingly illustrate that the work of a company's internal audit function can be used as much as a sword against a company as a shield to protect it.
- Effective internal audit departments perform crucial monitoring work to test whether a company's internal controls are operating as desired, and their findings guide remediation of identified issues. But when identified issues are not appropriately and promptly taken up by management, prosecutors and regulators may use these findings—often contained in non-privileged reports—to evidence corporate compliance program deficiencies, for example:
  - Failure to respond to issues identified by internal audit;
  - Failure to address critical-risk and high-risk deficiencies; and
  - Failure to improve inadequate compliance controls at acquired companies.

> 6. Prior to 2010, Quad was a privately held printing company headquartered in Sussex, Wisconsin, with a focus on domestic sales. With the July 2010 acquisition of World Color Press, Inc. ("World Color"), a Canadian printing company, Quad quickly became a public company with a major international presence. Quad acquired over 16,000 World Color employees, several subsidiaries, and multiple plants throughout Latin America, and its common shares began trading on the NYSE. Despite becoming a publicly traded company with a large global workforce and operations in high risk areas, Quad's compliance program was almost non-existent in 2010. At the time, Quad failed to implement sufficient internal accounting controls or anti-corruption policies and procedures and failed to conduct meaningful due diligence on third parties. Likewise, internal audit had no visible role in anti-corruption testing and the company failed to conduct broad FCPA or ethics training until approximately 2012. It appointed its first Director of Compliance, an individual with no compliance experience or training and an information technology background, in 2011.

[Quad/Graphics, Inc. SEC Order (Sept. 26, 2019)]

- Companies accordingly must ensure not only that their internal audit functions are effective, but also that management is equipped to respond effectively.

Compliance Trends to Watch in 2020

- ***Cybersecurity and Data Privacy:*** These issues are here to stay and will inevitably become increasingly significant.
- ***Gatekeepers:*** Gatekeeper liability will remain a focus and government authorities will continue to treat gatekeeper involvement in misconduct as an aggravating factor. Companies will be expected to provide appropriate support to gatekeepers.
- ***ESG:*** Environmental, social, and governance efforts and disclosures will be priorities for both stakeholders and regulators; attention to these issues is an imperative.
- ***Consolidating Compliance Expectations:*** Regulators' compliance expectations are becoming increasingly aligned in certain areas (e.g., sanctions, national security, and FCPA), and this is likely to continue—although continued growth of multi-jurisdictional matters will require dexterity in navigating different regimes and regulatory expectations.

GIBSON DUNN

Upcoming Gibson Dunn Webcast & Today's Panelists

Upcoming Gibson Dunn Webcast

February 11, 2020 | 12:00 pm – 1:00 pm EST

German Corporate Sanctions Act

Panelists: Finn Zeidler (Frankfurt) and Ralf van Ermingen-Marbach (Munich)

To Register, Click Here

German criminal law so far does not provide for corporate criminal liability. Corporations can only be fined under the law on administrative offenses, and the government has discretion to impose such fines.

In August 2019, the German Federal Ministry of Justice and Consumer Protection circulated a legislative draft of the Corporate Sanctions Act which would introduce a hybrid system. The main changes would eliminate the prosecutorial discretion in initiating proceedings, tighten the sentencing framework and formally incentivize the implementation of compliance measures and internal investigations.

Join our team of German white collar lawyers for a discussion of what companies can expect regarding corporate crimes enforcement. Topics to be covered:

- Farewell to discretion - Mandatory prosecution of corporate crimes
- New sentencing framework - Imposing harsher sanctions
- Legal incentives for compliance, internal investigations and cooperation
- Statutory requirements for internal investigations
- Protecting documents against seizure

Today's Panelists - Contact Information

F. Joseph Warin

Partner
Washington, D.C. Office
Tel: +1.202.887.3609
FWarin@gibsondunn.com

Zainab Ahmad

Partner
New York Office
Tel: +1.212.351.2609
ZAhmad@gibsondunn.com

Stuart F. Delery

Partner
Washington, D.C. Office
Tel: +1.202.887.3650
SDelery@gibsondunn.com

Michelle M. Kirschner

Partner
London Office
Tel: +44.20.7071.4212
MKirschner@gibsondunn.com

Adam M. Smith

Partner
Washington, D.C. Office
Tel: +1 202.887.3547
ASmith@gibsondunn.com

Lori Zyskowski

Partner
New York Office
Tel: +1 212.351.2309
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
2001 Ross Avenue, Ste. 2100
Dallas, TX 75201-2923
+1 214.698.3100

Denver
1801 California Street
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

Frankfurt
TaunusTurm
Taunustor 1
60310 Frankfurt
Germany
+49 69 247 411 500

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

Houston
811 Main Street, Suite 3000
Houston, TX 77002
+1 346.718.6600

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